Title : A strategic framework for e-government security: the case in Nigeria

Name : Sam Neekpoa Deekue

A STRATEGIC FRAMEWORK FOR E-GOVERNMENT SECURITY- THE CASE IN NIGERIA

SAM NEEKPOA DEEKUE

PhD

2016

UNIVERSITY OF BEDFORDSHIRE

A STRATEGIC FRAMEWORK FOR E-GOVERNMENT SECURITY-THE CASE IN NIGERIA

BY

SAM NEEKPOA DEEKUE

A thesis submitted to the University of Bedfordshire in partial fulfilment of the requirements for the degree of Doctor of Philosophy

April, 2016

Abstract

Countries across the globe are striving towards full-scale implementation of e-government. One of the issues arising with the efforts to this realization is the assurance of secure transactions while upholding high privacy standards. In order to engage citizens in the process, there must be transparency and confidence that the e-government systems they are using are reliable and will deliver the services with integrity, confidentiality and accountability. Different systems require different levels of security according to the services they provide to their users.

This research presents an investigation into reasons why e-government security frameworks developed by researchers with the claim that it is one-size-fits-all issue may not hold true, particularly in the case of Nigeria, based on certain identified realities.

The claim of a generalized framework appears very challenging because there seem to be much diversity across different governments. Countries differ in one or more of the following characteristics: political systems, legal systems, economic situation, available technological infrastructure, Internet and PC penetration, availability of skills and human resources, literacy levels, computer literacy levels, level of poverty, leadership, and ethnic diversities in terms of norms, languages, and expertise.

Security measures implemented in e-government projects in some developed countries, beginning with more established e-government systems around the world, were evaluated and a strategic framework for e-government security proposed which considers both technical and non-technical factors that involve people, processes and technologies.

The framework is proposed to advance the rapid adoption of practices that will guarantee e-government security. It seeks to provide a flexible, repeatable and cost-effective approach to implementing e-government security. This research examines the issues of enclosure in the implementation of e-government from the perspective of security and ultimately survivability.

Declaration

I declare that this thesis is my own unaided work. It is being submitted for the degree of Doctor of Philosophy at the University of Bedfordshire.

It has not been submitted before for any degree or examination in any other University.

Sam Neekpoa Deekue

---------- ----------

Name of candidate Signature

Date

Dedication

I wish to dedicate this work to the loving memory of my beloved mother

Lady Barikpoa Sam Deekue

Table of Contents

List of Tables

List of Figures

List of Abbreviations

CA	Certificate Authority
CIA	Confidentiality, Integrity and Availability
COBIT	Control Objectives for Information and related Technology
G2B	Government to Business
G2C	Government to Citizen
G2G	Government to Government
ICT	Information and Communication Technology
ISO	International Organization for Standardization
IT	Information Technology
MDAs	Ministries, Agencies and Departments
NIST	National Institute of Standards and Technology
NITDA	National Information Technology Development Agency
OECD	Organisation for Economic Co-operation and Development
PDCA	Plan-Do- Check-Act
PEOU	Perceived Ease of Use
PKI	Public Key Infrastructure
PU	Perceived Usefulness
SFS	Security File System
UNDESA	United Nations Department for Economic and Social Affairs
UNPAN	United Nations Public Administration Network

Acknowledgment

I do thank the almighty God for his special grace and enablement through the period of my PhD. The period of the research was not without some forms of challenge, but I completed it successfully due to the consistent supervision of my Director of Studies, Dr. Xiaohua Feng; she gave unfettered access to her office and all to give me the required direction regarding my research. I also appreciate Dr. Enjie Liu, my second supervisor, for the valuable professional advice throughout the period of the research.

My heartfelt appreciation goes to members of the SAM-DEEKUE dynasty: Sir Sam N. Deekue (JP), Engr. Louis Sam-Deekue, my vivacious Princes and heirs, Wesley and Jeffrey Sam-Deekue. A very special gratitude to my loving and caring wife Barr (Mrs) Beauty Sam-Deekue for her special support, care and understanding all through the period. I was greatly motivated by the love, trust and high expectation from members of my family.

I cannot have this opportunity and not express my very sincere appreciation to my most special friend Mr. Edward Eresu Deekae for his consistent support and encouragements, special acknowledgement to my friend and personal staff, Mr. Mene Naanee, who gave me a great deal of support during the period: he handled my personal businesses while I was away for studies. A special acknowledgement to Bro Solomon Kwaku, Bro Emma Ogbesaniwu, Pastor Nick and Pastor Debbie Egbaran and members of Christ Embassy and all the staff members of Wes-itec Limited.

Lastly, my thanks to Dr Peter Norrington for assistance with proofreading.

May the blessings of the almighty God rest upon you all richly.

Introduction

Background to the Research

The world of information and communication technology (ICT) and the need to transmit data swiftly and efficiently has determined a continuous evolution of network technologies leading government agencies and departments to make available their private network applications, core administrative services, and customer-related information to business partners and employees. E-government concept is to make these applications and services easily accessible to citizens 24 hours a day, 7 days a week, no matter how remote your location may be.

E-government is the utilization of information and communication technologies, like the Internet services and other data networks by government establishments to carry out its functions. Its deployment is changing the fundamental relationship between government and citizens and thereby improving the government's service delivery, as a result achieve a novel way of accessing government information (Boudriga, 2002). The primary modes of delivering e-government are in different categories: it could be government to citizens (G2C), government to business (G2B) or government to government (G2G). The understanding that e-government is more convenient as well as cost-effective for businesses has made government all over the world to consider its adoption, citizens also derive immense benefit because they can now have very easy access to current governmental information without travelling or dissipating so much energy.

This online platform has provided an opportunity to all public sector organisations, to modernise and bring about citizen-centred services by putting together integrated policies and programmes that will drive efficiency across government departments and agencies. Though a lot of countries have fully implemented e-government while others have only implemented it in part, some of the countries only plan to electronically transform the main administrative processes as it were without major technological improvements.

E-government is expected to simplify bureaucratic processes and make access to government services swift for all legitimate businesses and citizens. It is supposed to be more efficient than the traditional process, improve accessibility to civic services with transparency and accountability (Tsui et al., 2010).

The methodical mission to integrate data that will enable government to benefit from the economy-of-scale, to enhance data repository services, and cut down cost of government transactions are undeniably logical reasons to make an investment in e-government by any government around the world (Andersen & Henriksen, 2006).

E-government primarily started as a process whereby government agencies built websites and started uploading information about government programs and services, and was basically meant to inform the public of its activities. It was used as a government tool for information dissemination, after which it progressed towards processing other more critical transactions online. Then later government carried on continually to the point of engaging citizens online in a way that encouraged citizen's participation without restriction of time or location, it offered services that enabled citizens and businesses to link up with public functionaries through the Internet (Schwester, 2009).

It took advantage of IT tools like the wide area networks, the Internet and mobile phone to better the communication methods between government and citizens (Basu, 2004). E-government fundamentally makes government smarter and less cumbersome, its aim is to improve the way government delivers its services and provide the public with better way of interacting with the authorities.

In as much as we have found several descriptions of e-government, most academics and stakeholders defines it as government application of information communication technologies to provide citizens and businesses with the prospect of interacting and conducting businesses with government, through the use of various electronic media like the mobile phone, self-service kiosks and the Internet (Almarabeh, 2010). It is basically a utilization of ICT to improve effectiveness, build a

transparent and accountable way of carrying out government transactions (Moosa & Alsaffar, 2008).

E-government is considered one of the great advancements in the field of information technology; it actually has provided a sophisticated opportunity for the reinvention of government processes.

According to Moosa et al. (2008), "It promotes transformation from traditional bureaucratic paradigms, that are agency-centric and lays emphasis on standardisation, departmentalisation, fragmentation and operational cost-efficiency. The e-government paradigm is customer-centric, lays emphasis on synchronized network building, external co-operation and customer services" (Moosa & Alsaffar, 2008, p.52).

It is not just about putting in computers or building a website for information access; it is about transforming the fundamental connection between the government and the citizens (Zhang, 2010). The main purpose of e-government is the efficient delivery of government services and programmes to citizens.

Research Aim and Objectives

Aim

To develop a strategic framework for e-government security that will sustain uninterrupted service delivery to users regardless of underlying system deficiencies.

Objectives

- To carry out critical study of existing academic research on e-government security implementations.
- To present a theoretical and conceptual framework for secure e-government research.
- To verify primary reasons for the slow pace of e-government adoption in Nigeria and recommend a solution.
- To check compliance with existing standards, frameworks and best practices.

- To build a strategic framework for e-government security implementation in Nigeria, that will consider every aspect of e-government security, the people, the processes and the technology.
- To integrate a fault-tolerant mechanism to guarantee survivability in the e-government security system.

Research Motivation

After three years of work as an executive in one of the local government authorities in Nigeria, I realized that a lot of man hours were spent on simple transactions and this was adversely affecting overall productivity of local government. The solution that came to mind was the introduction of an IT-based system that will manage the internal communications of the council first, before thinking about introducing it to the public. At the time, reports had it that e-government was still considered to be at its embryonic stage in Nigeria. As I continued to search for more information about the operations of e-government, several reports emerged bolstering the inherent advantages of deploying e-government services to the people. It was claimed to enhance transparency in governance and be more convenient for citizens to carry out civil transactions with government, which apparently will reduce the long queues in offices for matters that could be sorted by just filling an online form at any time from any location.

However, as fantastic as the advantages were, there were several potential dangers when in operation. These downsides might be responsible for why the public and the government responded somewhat slowly to its adoption.

I was motivated to carry out an investigation, interviewing top government functionaries, and academicians as well as the general public on the probable reasons for the present level of e-government in the country. The technology has proven to be credible; why was the pace of adoption slow? I knew there was a need for a thorough study in the area. Whatever the problems were, they could be solved. The first aspect of the study was to investigate causal effects and the second part was to provide a solution to the problem.

While I disagreed with Choi and Chun (2013) that claims that the security framework that was built for South Korea could be applicable to all countries, I supported the argument of Rabaiah et al. (2009) that one size cannot fit all. Countries differ significantly in several ways and therefore, there will be diversities in the strategy and control of e-government security according to identified peculiarities.

As demonstrated in this research, the peculiarities of Nigeria were identified in the design of a novel security strategy for e-government implementation.

Research Questions

The realization of e-government projects does not depend only on government policies, but depends largely on citizens' readiness to trust and adopt it as a means of transaction (AlAwadhi & Morris, 2009). The developed countries have been enjoying e-services for a long time. Though, the developing countries including Nigeria were still struggling with the processes (Alateyah et al., 2013b). What were the likely factors responsible for this slow pace of adopting e-government, Nigeria in particular? Adoption is a significant characteristic to achieve a successful e-governance structure.

According to Alateyah et al. (2013), how does government intend to make the citizens embrace the use of e-government applications, when there is little or no research in exploring determinant factors that influences the adoption of these services by citizens in the less developed economies of the world. What are the existing scientific or conventional methods to improve the adoption of e-government by citizens? Can there be better implementation strategies or frameworks that could deal with the real concerns of citizens as regards e-government adoption?

Top policy makers, may definitely need to understand necessary requirements that may promote the use of e-platforms as against the traditional means of delivering government services (AlAwadhi & Morris, 2009). The research work presented in this thesis addresses the study objectives through the following research questions:

1. What are the relative preferences between e-government transactions and the traditional manual way of conducting government businesses?
2. What is the present maturity level of e-government development in Nigeria, in line with the United Nations Maturity Model?
3. What is the acceptability or satisfactory level as regards the current level of e-government development amongst stakeholders?
4. What is responsible for the slow pace of e-government adoption in Nigeria with reference to the latest rankings by the United Nations e-government development survey?
5. Is unique identification of citizens relevant to e-government deployment in Nigeria?
6. Is it vital to integrate a security framework into an e-government strategy from the outset?

Research Limitations

The researcher was not in control of legislative and policy direction in the case study; however, a framework is expected to comply with relevant laws and policies of a state. At the time of the research some laws related to cyber security were passed though policies on enforcement were still unsettled. Therefore, the study could only base its projections on the existing state of affairs, which are subject to change as government policies are never static.

Access to every stakeholder could not have been possible given the population of the country; hence a valid sample was used to carry out the study at the most competent level.

The researcher observed some bias amongst civil servants while responding to questionnaires: some of them for the purpose of shoring up the image of the administration tended to present a positive representation to a situation that apparently was not the reality, even though the research was strictly academic.

The scope of the research was not to deploy an e-government system but to provide a strategic framework that could be extended in the future research.

Thesis Outline

Chapter one – provides background information on the study, describing the importance of the subject. It states the research objectives, research questions, motivations and significance.

Chapter two – reviews existing work in the field of e-government adoption and information security. Starting from historical background, theoretical models, frameworks and empirical literature related to the study of e-government security; the chapter expounds upon critical barriers in the implementation of e-government, hypothetically stating that security and privacy is about the most important concern in the adoption of e-government amongst stakeholders. The chapter reviews security requirements and policies in relation to e-government implementation.

Chapter three – defines key factors that brought about the supposition of this research; it gives an interpretative approach to the concept of e-government adoption within the confines of the case study. It examines factors such as the ranking of countries by the United Nations e-government survey in relation to Internet penetration in the country. The conceptual framework defines the levels of e-readiness in Nigeria, e-government initiatives and primary factors affecting the growth of e-government.

Chapter four – describes the exact steps that have been undertaken to address the research questions. It explains the types of research, the reason for adopting the approach and strategy, methods and techniques used to achieve the required evidence, as well as methods used for data analysis and validation.

Chapter five – emphasizes the need for the framework to be in compliance with relevant information security regulations, guidelines, frameworks, policies and best practices in the industry.

Chapter six – presents the proposed framework designed to advance the rapid adoption of practices that will guarantee e-government security; that will provide a flexible, repeatable and cost-effective approach to implementing e-government

security with special features of guaranteeing survivability through the utilization of a fault-tolerant mechanism.

Chapters seven – conclude the research, provide a summary of key findings, and make recommendations for future research.

Literature Review

Introduction

This chapter gives insight into relevant areas of this study; with the introduction to basic concepts of e-government and practices, e-government maturity stages and its maturity models. Issues related to e-government adoption are very critical in both developed and developing countries, so situating this adoption in line with contemporary United Nations e-government ranking is crucial. This chapter expounds upon critical challenges facing e-government adoption, realising that security and privacy is one of the major concerns in the adoption of e-government amongst stakeholders. What are the existing security strategies or frameworks designed to guarantee e-government security both in developed and developing countries were highlighted while further details are discussed in subsequent chapters.

E-government Background

As stated earlier, Schwester (2009) reported that e-government primarily started as a process whereby government agencies built websites and started uploading information about government programs and services, and was basically meant to inform the public of its activities. It was used as a government tool for information dissemination, after which it progressed towards processing transactions online. Then later government carried on continually to the point of engaging citizens online in a way that encouraged citizens' participation without restriction of time or location, it offered services that enabled citizens and businesses to link up with public functionaries through the Internet (Schwester, 2009).

It is the utilization of information technology tools such as the Internet to carry out traditional government services with the aim of transforming the relationship between citizens and government (Basu, 2004). The bureaucratic processes in government most times could be so unwieldy, making citizens to want to cut corners, but e-government helps to make the processes easier, convenient and

simple. It makes public services more accessible to the people while guaranteeing transparency and accountability (Tsui et al., 2010).

The Concept of E-government

In as much as we have found several descriptions of e-government, most academics and stakeholders defines it as government's application of information communication technologies to provide citizens and businesses the prospect of interacting and conducting businesses with government, through the use of various electronic media like the mobile phone, self-service kiosks and the Internet (Almarabeh, 2010). It is basically a utilization of ICT to improve effectiveness, build a transparent and accountable way of carrying out government transactions (Moosa & Alsaffar, 2008).

E-government is considered one of the greatest advancements in the field of information technology; it actually has provided a sophisticated opportunity for the reinvention government processes.

It is not just about putting in computers or building a website for information access; it is about transforming the fundamental connection between the government and the citizens (Zhang, 2010). The main purpose of e-government is the efficient delivery of government services and programmes to citizens electronically.

Significance of E-government

E-government implementation may give rise to significant outcomes by providing more efficiency in governmental transactions, improve easy accessibility to services, ensure accountability and transparency in governmental processes and reduce cost and man-hour involved in carrying out government services, leverage on market forces to enhance the relationship between government and citizens (Gupta et al., 2008). E-government appears to be more convenient for users, although citizens may not be very patient to learn how to use some of the applications when they are introduced to the public.

Putting together an e-government strategy can be of great significance to the overall processes of designing and implementing e-government for better service delivery (Alshehri & Drew, 2010). According to Alshehri et al. (2010), the Organisation for Economic Co-operation and Development (OECD) carefully studied projects within it members and outlined the benefits of adopting e-government services: the advantages that were identified are as follows:

- It improves effectiveness in processing large form of data
- It enables stakeholders to share data, therefore making it possible for the achievement of specific policy outcomes
- Enhances productivity which in turn facilitates government economic policy objectives
- Contributes to governments' reform by improving transparency in governance
- It facilitates information sharing
- It helps engender trust between governments and its citizens

(Alshehri & Drew, 2010).

The emergence of the e-government system has made it possible for more convenient access. It could be in the form of unmanned kiosk in a public office building, or a service point situated at designated centres within towns and communities, or through the use of personal computers/mobile devices in homes or offices (Alshehri & Drew, 2010; Nkohkwo & Islam, 2013).

E-government is supported by regulations and policies of e-governance, bringing together IT governance and global governance, as well. E-government can be said to be beneficial to both rich and poor countries alike. It can be an especially powerful and important tool for cities in developing countries. These cities face a number of challenges ranging from poor public services, unemployment, lack of housing, crime and violence, and in other areas such as health and education, which will only be more arduous as cities grow in population. It can also advance local democracy by improving access to information and deepen citizens' involvement in the decision-

making process; it opens new opportunities for cities and local governments to engage in governance by requiring reforms of underlying working processes.

It is a little bit difficult to quantify all the advantages of e-government implementation, because as citizens and government continue to use it, the inherent benefits in the e-services become more apparent. The many errors associated with governmental processes are reduced if not eliminated with the introduction of e-transaction, citizens input their data through the web and it goes directly to the backend without human intervention. It seems as though citizens are in temporal employment of government as they spend few minutes of their time to complete online forms or applications at a time convenient for them. E-government enables the simplification of government processes (Marawar et al., 2010).

E-government Implementation

E-government is considered as about one of the greatest advancements in the field of information technology; it could be classified as a transaction between governments and government agencies at the federal, state or local government levels (G2G), government to business (G2B), or government to citizens (G2C) (Moosa & Alsaffar, 2008).

According to Weerakkody et al. (2012), though the purpose of e-government is similar for every country, the strategies, modes and resources for implementation may not be the same base on peculiar circumstances.

Similar to other information technology based initiatives, to implement viable e-government system, it will require the co-operation of relevant stakeholders to pull resources together, streamline diverse viewpoints to breed a common ground. These viewpoints are sometimes different forms of technology, interest or artefact. It is important that every contending interest be acknowledged and considered thoroughly in order to achieve set objectives (Azad & Faraj, 2008)

The ***stakeholders*** of e-government could be individual member of the public or corporate organisations, designated staff of government, government consultants

or contractors (Alharbi et al., 2014). Principally, e-government can be classified into the following subsections:

Government to Government (G2G)

This is an internal communication between government establishments, department to department, agency to agency. Every internal mechanism must be perfected before transacting with those external to the system. It is programmed to work according to the rules governing civil service but in a modernised form. An example is inter-agency verification system like the police verifying a suspect's identity from the immigration service (Al Nagi & Hamdan, 2009). This inter-agency communication will help in crime detection and swift emergency response (Evans & Yen, 2006).

Government to Business (G2B)

This is dedicated to serve corporate organisations or business; the private sector cannot thrive without collaborating with the public sector. This collaboration is enhanced by the government to business engagement. This is direct line of communication for business entities to relate with government on issues of mutual benefit. Though everything will be done in line with established rules and regulations, this development encourages a more flexible and robust national economy (Al Nagi & Hamdan, 2009). Example of G2B services are: new company registrations, procurements, payment of taxes and licensing.

Government to Citizens (G2C)

The primary goal of e-government is to serve the citizens efficiently and effectively through innovative technologies. It can only be accomplished by improving the method of communication between citizens and government via the e-government platform. The interaction may be via government designated websites or contact numbers which apparently saves time than the traditional manual ways. The utilization of smart systems for user verifications makes everyone to access desired services irrespective of social status (Al Nagi & Hamdan, 2009). Examples of G2C

services are: drivers license application, international passport application, payment of council tax etc. It is vital for countries to promote citizen's adoption of e-government services because it requires very little effort to accomplish much.

Government-to-Employee (G2E)

This could also be referred to as intra-government communication, as it is concerned with transactions and processes that are essential to those within government employment. Issues that have to do with management of the employees' welfare, it could be staff training needs, payroll or pension (Al Nagi & Hamdan, 2009).

Dissimilarity between E-Government and E-Commerce

Strategically, a vital distinguishing issue between e-government and e-commerce is that government's main responsibilities are about the welfare of the people, and security of lives and property. For government to ensure a systematized quality of life for citizens, the principles are provided in several organisational and governmental records, also reflected in laws and policies. Whereas, in commerce the primary interest is directed towards profit-making (Wimmer & Bredow, 2002).

Also, the multiplicity of government functions requires different security procedures. Even though a number of theories for systematic processes in e-commerce may be applicable to e-government, the main business of government involves treating every case uniquely and adopting an individualized negotiating process as any person approaching government has an interest to protect. Therefore confidentiality is key (Wimmer & Bredow, 2002).

There seem to be more significant challenges in e-government than e-commerce due to the fact that government records are mostly protected by privacy laws which may not be the case in e-commerce, making government services highly confidential (Al-Khouri & Farmer, 2014). The nature of the information in an e-government transaction could be very sensitive than the e-commerce transactions, e.g. a patient's medical history if seen by an unauthorised person constitutes a

breach of privacy and data protection laws (Al-Khouri & Farmer, 2014). Another example, according to Al-Khouri & Farmer (2014), is the unauthorized disclosure of economic data which may impact the outcome of the stock markets, such consequences may be huge, therefore e-government initiatives must ensure that its framework is designed to guarantee excellent security standards (Al-Khouri & Farmer, 2014).

E-government Adoption Constraints

According to Nugi Nkwe (2012), there are several reasons why adoption of e-government may be slow, opinion of users of the applications must be sort through a survey or feasibility study. Corporate organisations may have some reservations about sharing their data online; they may wish to know how useful the new innovation will affect the fortunes of their business, how easy or convenient it will be for their business. It is very important to consider the belief system of citizens, most citizens are not always comfortable adopting new ideas, anything that seem complex they may want to avoid (Nkwe, 2012).

From available studies from different countries, there are many challenges and issues that need to be addressed for successful operation of e-government. There are divergent factors that influence the adoption of e-government, and these factors depend on the local realities of any country. Virtually, these barriers may have a significant effect on the development of government organisations' capabilities to provide e-government transactions. Other challenges include inadequate information technology infrastructure, security and privacy issues amongst others (Nkwe, 2012). Constraints to the adoption of e-government may differ from country to country; these constraints may delay the processes or affect the effectiveness of the deployment. Issues like inadequate IT infrastructure, limited human resources, knowledge gaps, insufficient funds, and concerns over security and privacy.

However, adoption of e-government may be classified into categories, the first category is the e-government supplier and the second category is the consumer.

The supplier here could be the federal, state or local government or its agencies. While the consumers are the citizens, corporate bodies, international and local organisations (Al-Hujran et al., 2015). Most of the studies available have concentrated on the constraints in the adoption of e-government from the supplier's perspective which were identified to be as a result of lack of IT infrastructure, insufficient funds, manpower to design a roadmap or policy.

On the customers side, citizens considers among other things, the usefulness of the e-government, will it be easy to use, level of IT education amongst citizens, security and privacy of personal data, issues of trust as well as quality of service (Al-Hujran et al., 2015).

Bélanger & Carter (2008) illustrated a situation in the USA, that funds earmarked for e-government projects were to increase by 6.9% annually but citizens tended to be more inclined to using the traditional ways of queuing up in offices to carry out government transactions. It was stated that despite the huge investment in e-government, if citizens do not have confidence in the system to protect their privacy, the entire e-government project will not achieve its desired goal as citizens may not patronise it (Bélanger & Carter, 2008). It is therefore vital to consider also the things that may affect customers confidence in the system, otherwise all the efforts and funds may be futile.

Barriers and Challenges

Table 2.1 summarizes the challenges facing e-government adoption as demonstrated by Alharbi et al. (2014) in an article titled: "Security Challenges of E-Government Adoption based on End Users' Perspectives".

Table 2:1 Challenges facing e-government adoption

S/N	Challenges	Example
1	Proficiency in the use of ICT	• Not every citizen or government employee is proficient in the use ICT facilities and applications • Users are not conversant with information security principles, therefore do not know what to avoid
2	IT Infrastructure	• Low bandwidth which may affect network throughput • Interoperability problems amongst applications • No routine updates for software and hardware, particularly security programs • Difficulty in database integration
3	Security issues	• No guaranteed privacy protection policy • When citizens don trust their political leadership, they tend not to trust its innovations • Concerns about the confidentiality of personal data • Lack of protection during the transition process • Concerns over the physical security of ICT equipments and Lack of trust in the Internet
4	Availability	• Unavailability of Services at the time of request • Insufficient protection of the services against Denial of Service attacks • Too much delays in service delivery as a result of network issues
5	Accessibility	• Limited access to channels for e-government users • Insufficient network coverage in cities and communities • Adequate provisions for disabled users accessing e-services
6	Lack of Awareness	• Insufficient security awareness amongst users • Exposure of personal information to unauthorized persons
7	Design of the Website	• Difficulty in understanding the web applications, difficult to use • Difficulty in navigating through the web sites
8	Cultural issues	• Unwillingness to adapt to new technology • Concerns over religious and tribes • Concerns over plurality of languages (language barrier)

One of the great hurdles frequently cited in the adoption of e-government is the need to guarantee sufficient security and privacy within an e-government strategy, realising that security is one of the most significant factors when considering online government (Ebrahim & Irani, 2005). Available literature posits that one of the biggest challenges of e-government is security, users may rather opt to continue with status quo instead of making use of an unsecured web application to conduct government transactions (Mohammadi & Nikkhahan, 2009). Some factors that may lead to breach of security and privacy could be as a result of incompetence on the part of staff handling software configurations, apart from threats from viruses and other malwares. Hackers or intruders may take advantage of the lack of strict adherence to security and privacy policies, fragile physical security to perpetrate their criminal acts.

E-government Maturity Models

To implement e-government there are existing models that stands as a guide, they are referred to as e-government Maturity Models (eGMMs). They were put together by researchers, international bodies and the academia for the purposes of providing guidelines and standards for the proper implementation of e-government applications (Karokola et al., 2013).

In measuring various levels of maturity, you may have to consider the scale of complexity of the technology to be used with how easy it could be for users to navigate. Table 2.2 highlights the various stages of maturity as described by different authors.

Table 2:2 E-government Maturity Models

Model Description	Maturity Stages	References
Two-Stage Maturity Model	cataloguing, transaction	(Reddick, 2004)
Three-Level Maturity Model	publishing , interaction, transaction	(Howard, 2001)
Four-Level Maturity Model	catalogue, transaction, vertical integration, horizontal integration	(Layne and Lee, 2001)
Five-Level Maturity Model	cataloguing and dissemination, of information dual communication, service & financial transaction, vertical and horizontal integration, political participation	(Moon, 2002)
Five-Level Maturity Model	emerging, enhanced, interactive, transactional, fully integrated	UN's five-stage model (2001)
Five-Stage Development Model	closed, preparatory, developing, controlled, seamless	Safari et al.(2004)
Five-Level Maturity Model	web presence, interaction, transaction, transformation, e-democracy	Siau et al. (2005)
Deloitte's Six Stages Model	information publishing/distribution, official dual-way transaction, multi-purpose portals, portal personalization, clustering of common services, full integration and enterprise transaction	Deloitte and Touche (2001)

After comparing the eGMMs, it became apparent that the design focus was principally on its functions and e-government service delivery than the quality of service therefore it is lacking some security features.

E-Government Stage Models and their Characteristics

Jayashree (2010) observed that e-government should not be regarded as a single process on integration of services. It could be described as an evolving process, connecting several steps or segments of maturity. A summary of the various stages of e-government maturity is presented here, to compare and contrast various

illustrations by the World Bank, the United Nations, the Gartner Group as well as other individual researchers (Jayashree et al., 2010).

1. The World Bank's three-stage model

Publishing: Developing countries generally commence their e-government processes by uploading government information on the website, starting with the publication of government rules, regulations, documents and forms. It may be different in design and content from country to country.

Interaction: E-government connects with members of the public with issues concerning governance processes by communicating with them through various interactive medium, discussing with top officials during the periods of policy drafting at every level. This may strengthen public engagement which eventually enhances public confidence in government.

Transaction: Government extends its effort through the building of websites that give opportunities to the public to carry out multiple transactions electronically, thereby improving productivity (Jayashree et al., 2010)**.**

2. The United Nation's five-stage model:

(United Nations Public Administration Network, 2013)

Emerging Presence: A designated or some websites belonging to respective government agencies may publish scanty official but static information.

Enhanced Presence: Websites belonging to government will publish official but dynamic information and updates them on a regular basis.

Interactive Presence: A designated website belonging to government connects the public and the service providers making a methodical communication between citizens and government.

Transactional Presence: Citizens can carry out a completely secure electronic transaction using a designated government website. It could be an application of a driver's license or tax payment.

Seamless or fully integrated presence: A designated government website as a one-stop shop for all government transactions, services are provided very seamlessly with ease, every government that is required can be carried out this singular website.

3. Gartner's four-stage model:

Web presence: At this stage, government builds a website to upload basic information to inform citizens.

Interactive: At this stage, citizens can interact with government via the web email

Transaction: Citizens can carry out a full transaction like the application of birth certificate electronically

Transformation: Here there is a total transformation of existing operations to a more efficient, integrated and unified service (Jadi & Jie, 2014; Jayashree et al., 2010)**.**

4. Deloitte's six-stage model

Information publishing: More information than normal are made available to citizens.

Official two-way transaction: Communication technologies like digital signatures are introduced by designated agencies in the interaction between government the public.

Multi-purpose portals: A designated portal is used to provide all governmental services to the public.

Portal personalization: Users are allowed to modify portals as required

Clustering of common services: To improve collaboration between government and the public, aiming to reduce intermediate processes between operations so as to offer more integrated and seamless service.

Full integration and enterprise transaction: The principal goal of providing coherent, integrated and specialized services to every customer according to individual requirements and preference (Layne & Lee, 2001).

5. Layne and Lee's four-stage model

Catalogue: The website basically delivers static information to the public. **Transaction:** The capabilities of the catalogue stage are improved upon by enabling citizens to complete processes like filling of online forms or applications.

Vertical integration: This stage seeks to transform governmental services instead of to automate it regular processes. To integrate governmental functions at all levels are its major objective, e.g. transforming the functional relations among the tiers of government.

Horizontal integration: The focus is to integrate all the functions from different systems so as to give the public a more integrated and flawless service**.**

6. Keng Siau and Yuan Long's synthesizing e-government five-stage model

Web presence: Very limited information such as vision and mission statements, opening and closing hours, public holidays, contact address, email address and phone numbers are published at this stage.

Interaction: At these stage new functions for enhance interaction between citizens and government such as search engine, application forms for download, email systems are introduced.

Transaction: Here there exist a complete electronic transaction between government and the public, financial transactions can take place.

Transformation: This stage is about the transformation of governmental services instead of to automate it regular processes. To integrate governmental functions at all levels are its major objective, e.g. transforming the functional relations among the tiers of government.

E-democracy: E-government tends to gradually revolutionize the ways by which citizens respond to matters relating to political decisions (Marthandan, 2010).

About every nation represented in the United Nation do operate governmental portals. This Information Technology development is as crucial as armoured tankers, warships and military crafts in any nation's department of defence (Wang, 2009).

An e-government tool enhances the economic fortunes of businesses and empowers citizens (Al Nagi & Hamdan, 2009), however some countries are yet to adopt e-government.

Countries all over the world are striving towards the realization of e-government but a major concern negating the endeavour to accomplish it is the guarantee of a secure transaction while upholding high privacy standards (Gamlo et al., 2009).

Security Description, Requirements and Classification

Based on the development and widespread utilization of information communications technologies and computer networks, information security has gained prominence contemporarily (Al-Kuwaiti et al., 2009). There are no specific definitions for security but generally, it could be defined as the protection of an entity from undesirable occurrences. In Information Technology it is based on principles of the confidentiality, integrity and availability of assets. For a system to be considered secure, it should guard against issues that will not compromise the integrity, confidentiality or availability of the system (Al-Kuwaiti et al., 2009). Consequently, the concept of security includes the safeguarding of system networks as well as every vital component from various inappropriate activities that may compromise the integrity of data outcomes.

Security furthermore involves anticipating potential threats to the system, which may arise from insider abuse of privileges or an intrusion from an outsider. Thus, it could be said that security entails several other considerations not limited to guaranteeing confidentiality, integrity, and availability. It is therefore advisable that

e-government systems should be built to be very resilient against attacks from the onset, not to provide security as an add-on to an already deployed system.

Another way of expressing the concept is the resilience of a system to any type of malicious attacks. It is worth mentioning that most legacy systems and networks are typically designed with security as an add-on feature instead of having it as an essential integral part of the system design which sometimes affects the proper implementation of security policies.

The purpose of setting up a security framework in an information system is for initiating measures not only to ensure confidentiality, integrity, availability but other attributes like authentication and non-repudiation (Al-Kuwaiti et al., 2009). Security controls are put in place to ensure the systems are hardened to resist, identify and respond to security threats whenever. This can be achieved by employing theoretical and practical methods like encryption and intrusion detection and prevention systems (Al-Kuwaiti et al., 2009).

E-government is expected to adhere to the basic theories of Information Security: Confidentiality, Integrity and Availability, referred to as CIA (Rorissa & Demissie, 2010). Figure 2:1 is an illustration of the theory of CIA that for every e-government resource, the principle of CIA must be guaranteed.

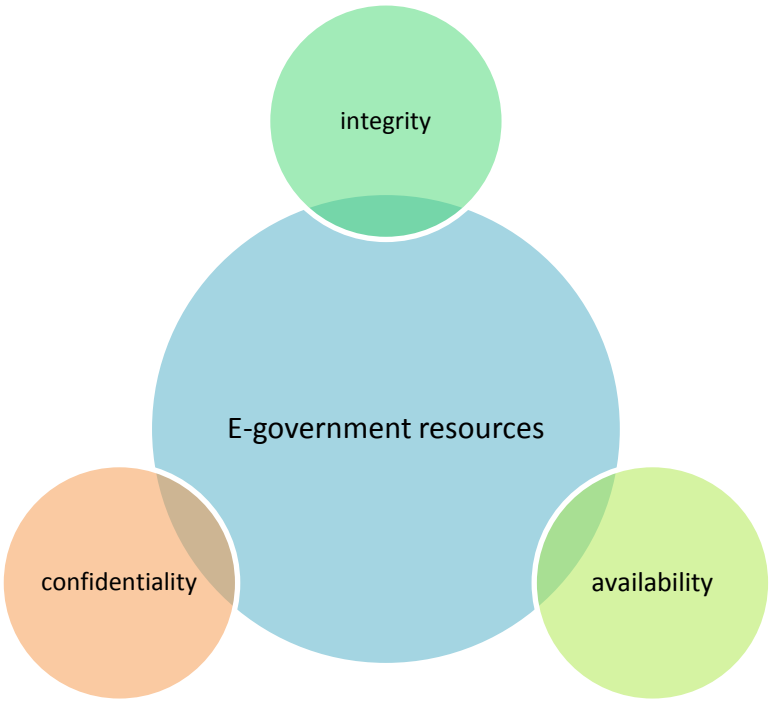


Figure 2:1 Confidentiality, Integrity and Availability CIA TRIAD

The above principle is regarded as the fundamental for any security framework as well as the factors for assessing a security system.

E-Government Security Overview

Security is perhaps the least understood aspect of information technology and business deployment (Boudriga, 2002). The premise of an e-government program is to offer an innovative way of accessing governmental services at anytime, anywhere over open networks. Reliance on this concept to deliver information and public services has increased amongst public sector agencies the world over. Now this growth has led to several inadvertent security concerns with countless new exposure to security threats (Omer et al., 2011).

To confront these challenges, governments have to build an efficient protection strategy. Security concerns have obviously affected the management of public services infrastructure (Omer et al., 2011). In the past, most organisations applied every possible precaution to make their facilities disaster proof, an approach

described as the fortress approach in defending their locations. Today, security has changed to become a critical infrastructure upon which entire new business applications are built and deployed. Security threats have never been more prevalent than they are today. Agencies, institutions, service providers and signal carriers have all experienced huge financial and service losses due to one cyber attack or another (Kalinich, 2013). Security plans, however, provide the enablement for government service providers to setup strategies to control the following issues:

Secure Messaging: Managing data passing through the network and preventing unauthorized modifications.

Authentication of Users: Ensuring that users are who they claim to be and providing integrity and non-repudiation of transactions.

Authorize Access to Sensitive Assets: Implementing mechanisms to make sure only authorized users have access to network resources at a particular time.

These security issues are commonly referred to as e-security. E-security is distinctly different from traditional security. This is mainly because the concepts and properties adopted do not operate only as a perimeter defence to government resources as in the case of traditional security (Boudriga, 2002), they analyse possible risk and makes a report (Butler, 2009)

Some of the security related issues in e-government service involves the identification and verification of users, storage and classification of citizens data on secure web servers, signing and certificate authorization, audit, conflict resolution and data backups (Omer et al., 2011). An e-government security system is expected to possess the capacity for multiple layers of authentication, ability to issue and revoke credentials, provide system audit, resolve conflicts, ensure accountability and availability, guarantee platform independence, ensure data integrity, maintain anonymity of users (Omer et al., 2011).

The pace at which e-government advances in development, deployment and use, and its infrastructures are quicker than the advancement and implementation of

the security components and other related considerations. This lack of security deployment is affecting both the services providers and the citizens alike.

Hacking for monetary profits or political advantages has continued to increase, prompting users not to regard it as mere mischief. The modes of attack are changing by the day, new attack techniques are created to outwit technologies like antivirus, system firewalls, intrusion detection and prevention systems (Walsh, 2014).

Consequently, it has become imperative to inculcate security strategies into the e-government system from the outset, from planning stage to implementation stage. It should not be done as an afterthought after the system has already been fully developed. As a matter of fact, as e-government contributes positively to national development, it could expose the country to great risk if not properly managed.

Government agencies need to be in control of securing their critical assets and information, even though security controls may require huge financial investment. It has become very essential to study the techniques of providing adequate privacy and security protection for e-government services proportionately because too much security as well could hinder optimum productivity (Setiadi et al., 2013).

Security issues are considered as the main framework to ensure the successfulness of any e-governmental proposal; if there is any security vulnerability, the whole system will be at risk (Alsultanny, 2014).

It has been observed that citizen's concerns about information security may constitute a negative impact on the response of customers to the e-government project.

Purpose and Role of Information Security in E-Government

According to Kay Fielden (2010), the Internet has gone past it initial boundaries and purpose now extending and exploring new frontiers in education, commerce, government and to every sector of the economy. Computer security and information security are often used interchangeably and erroneously too. Though

they are closely related and share a common objective of ensuring the principles of integrity, confidentiality and availability are maintained; nevertheless, there exist slight distinctions between the two (Sattarova Feruza & Kim, 2007). These distinguishing factors are basically based on their approaches regarding any issue, the techniques or methodology adopted and the focus. Information security considers the confidentiality, integrity and availability of data in transit or in storage irrespective of whether it is stored as electronic file in a system or a manual document shelved in a file cabinet. While computer security is about the continuous availability of computer applications and facilities, the data stored on the system is not its primary concern (Sattarova Feruza & Kim, 2007).

With the growing spate of cyber security, it implies that the financial implication for information security will have to contend with other software development costs. Software-development project managers need to be able to weigh up the possibility of a security breach and the corresponding effect of such security breach in making cyber security budget. The Organisation for Economic Co-operation and Development (OECD) Seoul declaration in 2008 asserted that providing adequate security for online services is a paramount responsibility of government globally. Cyber security has become central to global discuss on security and privacy, if a nation is exposed to threat to national security, it remains imperative to put in place an all-inclusive general cyber security strategy that will involve all the national security agencies and law enforcements. Fielden (2010) observed that the society requires the Internet to perform day to day functions for the overall good of humanity; saying that the Internet has really revolutionize the way information is shared globally.

There is urgent need to control electronic espionages and hi-tech crimes across the globe. Cyber-terrorists of recent times strategically target sensitive data in storage, and exploit vulnerabilities in systems.

Information and financial crimes are realities that require a more proactive and sophisticated strategy to manage. International organisations like the “OECD and the United Nations struggle with the sheer dimension and complex nature of a

global cyber security framework" (Fielden, 2010, p.26). Different levels of security protection are required to secure national and international information systems.

Governments, large corporate organisation, banks, military, health institutions, and small businesses accumulate huge sensitive personal data of clients, staff, commodities, research data and financial report. When this information is put together, put in storage or in transit. If any sensitive business or financial data is unlawfully disclosed to unauthorized persons, it is a data violation that may ruin a business, lead to litigation or make the business go bankrupt. The protection of confidential information is a requirement in business, it is also an ethical and statutory requirement (Sattarova Feruza & Kim, 2007).

E-government and Information Security Policies

Information security is directly connected to the concept of e-government security, it is used as a foundation for e-government security (Setiadi et al., 2013). Every e-government initiative will always be susceptible to security attacks if there are no proper security policies or strategies (Singh & Karaulia, 2011). Information security policies remain the cornerstone of information security efficiency. A security policy is proposed to describe what is required of any party as regards security of information systems.

The general aim is to manage human behaviour as an effort to minimise threats to system resources either inadvertently or intentionally. Information security policies provide strength to the security of information assets. Controlling sensitive information from accidental or malicious alterations, disclosure is the main requirement for ensuring data security. To discover the main elements of e-government security, basic information security components must be considered which consist of: physical security, logical security and administrative security (Setiadi et al., 2013; Singh & Karaulia, 2011).

Security Policy

High technological innovations may be ineffective in the absence of corresponding managerial prowess; it will be an error to think that the success of an attack is consequent upon the sophistication of technologies deployed by the attackers. Most of the time, it is not the technology involved but the loopholes in human management of risk factors (Trcek, 2003). Security policies are about the organisational procedures in the management of security processes. It is very fundamental to have security policies initiated by the highest level decision-makers in a particular organisation. A policy document may contain information security objectives, terms, scope, principles and practices, standards and guidelines, compliance issues, responsibilities as well as references (Trcek, 2003).

Example of an information security standard in this regard is BS7799 (BSI, 1999), it was recognised as an international standard (ISO, 2000) (Department of Trade and Industry, 2000). Therefore it is very important that organisations observe correctly these standards systematically for establishing its security policies.

The International Organization for Standardization (ISO) defines information security as the protection of confidentiality, integrity and availability of information; including essential properties like authentication, accountability, non-repudiation and reliability (Setiadi et al., 2013).

Fundamentally, all the definitions of information security mean defending information and system resources against threats or attacks. The 3 key objectives in information security are confidentiality, integrity, and availability, commonly known as the Confidentiality-Integrity-Availability (CIA) triad. The CIA triad can basically be explained as follows:

> **Confidentiality:** Information could be said to be confidential when it only accessible to authorized recipients at any given point in time, if for any reason the information is disclosed to the public without due authorization then the confidentiality of that information has been breached (Singh & Karaulia, 2011).

Integrity: Information can be said to have integrity when the information is intact from source to destination without any modification or deletion. Modifications of a document can be effected by an authorised person but not an unauthorized person or action (Singh & Karaulia, 2011).

Availability: Ability to access relevant information as at the time and place you need it (Setiadi et al., 2013).

There are also other vital components of information security that must be observed for complete information security management. They are Authentication, Authorization and Non-repudiation:

Authentication ensures proper verification and identification of the system users.

Authorization ensures that the right user is granted the right access.

Non-repudiation ensures that users are not able to deny an action that was taken or any transaction(s) they have carried out (Gamlo & Bamasak, 2009).

Threats to Information Security of E-government

These threats could come in different guises; they could be either internal factors or external factors. Traditional paper-based transactions face threats from both internal and external factors as well. E-government can be said to have inherited it, however internal threats basically come from human factors within an organisation (Zhao, 2011). Factors that may not be under the control of the providers of the e-services such as natural disasters, professionals with criminal intents (hackers), opponents to a government as well as terror groups all which constitutes external threat to e-government.

Irrespective of the assertions presented above on the common threats faced by both manual and electronic government, threats to e-government are always changing as the technology evolves, attackers are innovating advance methods of carrying their attacks (Zhao, 2011). The extent of exploitations may include cyber

stalking, invasion of personal privacy and unauthorized access to personal information (Reddick, 2010).

> "Sophisticated and coordinated denial of service attacks and zero day exploits represent an on-going threat. Any technological weakness could be exploited to control or deface and disrupt e-government web services or steal sensitive data. Social engineering attacks, legal exploits and phishing attacks represent a significant threat as well" (Al-Mayahi & Mansoor, 2012, p.203).

Weaknesses in the network security or application security could give room for privacy issues such as identity theft, access to citizen's credit card details, and all services that involve electronic money transfers (Al-Mayahi & Mansoor, 2012). There are several new technologies available to guarantee efficient deployment of e-government, but what appear to be more important are processes or mechanism that will enhance transparency and citizen's trust in e-government services.

The successful implementation of e-government security systems in relevant government establishments is very essential in protecting system resources so as to achieve assurances that these resources will be effectively safeguarded against incessant threats. It will be able to sustain an effectual and all-inclusive framework for determining threats to information security, while identifying and administering appropriate controls, and evaluating its efficiency.

Evaluating threats is a key aspect of e-government risk analysis. Giving priority attention to threat identification is actually the right direction for a security strategy as it will reduce the chances of neglecting key areas of risk that might otherwise remain vulnerable. Threats can manifest in various forms; in order to achieve its set target, a security strategy must be very comprehensive to deal with major threats. One must be sure that the right steps are taken against these threats (Rhodes-Ousley, 2013).

Security and Convenience

It was stated by Liu (2010) that the main focus of e-government security application is its ease of use or what you may call convenience for the authorized users. Most times in a bid to fortify an application it becomes very complex to use, difficulty in manoeuvring the application may not necessarily mean reliability. Recent studies show that a number of security solutions are way too sophisticated for users, thereby making the e-government application clumsy and ambiguous. Adequate security of information entails that the right person gets the right information without losing any part of the content. Liu (2010) in his paper also indicated that e-government security was a quandary without straight forward answers; and therefore argued that stakeholders must keep away from developing e-government in a hurry as there are no absolute security for any system, hence a balance between security and convenience is obligatory.

Security Analysis and Design

When carrying out a security project, it is pertinent to note the state of security in that particular government establishment and be acquainted with requirements from the security system and the plans to accomplish it through a security analysis and design process (Zuccato, 2007). Then this information should be connected to achieve an understanding of how a secure system can be actualized.

Consequently, it is important to give priority to requests in accordance with various degrees of significance and achievability (Zuccato, 2005). Subsequent to the realization of the importance of the demand for emphasising the aim of security analysis is to surmount uncertainty and redundancy of security requirements by translating them into codes understood by the programmers.

Thomas Combas et al. (2016) recommend the publications by the National Institute of Standards and Technology (NIST) in the assessment of security and control measures in the Risk Management Framework of top government organisations. It was demonstrated in the framework designed for the US Department of Defence in their paper “Integrating cyber security into NAVAIR OTPS acquisition” (Combass &

Shilling, 2016). Skopik et al. (2015) also acknowledged the importance of the NIST cyber security framework in the formulation of national cyber security policies in their paper titled “Establishing national cyber situational awareness through incident information clustering” (Skopik et al., 2015). Collier et al. (2014) agreed that the NIST cyber security framework nucleus is very effective and comprehensive, though they described it as somewhat overwhelming due to its numerous categories and subcategories.

Summary

The reason for having a background review of this study was to ensure that issues such as the maturity models and stages were adequately couched. Consideration of the place of information security in e-government, its requirements and classifications, as it affects the deployment of e-government. A major characteristic of e-government is Ease of Use: any e-government security strategy that provides adequate security but makes the e-government application complex to operate has failed to provide the required convenience which is a key fundamental of e-government. A good trade-off between information security and service convenience need to be considered when developing e-government security strategy.

Conceptual Framework of the Study

Introduction

This chapter discusses the researcher's perception of e-government development in the world in relation to the case study. First by considering available data by authorities such as the United Nations E-government Development Index as reported in its biennial reports; Internet usage report of countries around the world on the development of e-government; as well as countries' income levels with regard to the development of e-government. All of these were used to verify the level of e-readiness in Nigeria with the aim of identifying the unique challenges regarding e-government development as reflected by Nigeria's ranking amongst other countries in Africa and indeed the world. What conditions necessitated the present level of e-government development in Nigeria?

Factors that may influence Citizens to use E-government Services

Every responsible government strives to increase the quality of services delivered to citizens, however the success of any of such initiatives like e-government is not dependent on government alone. It requires the willingness of the public to make use of the services offered through e-government platforms, therefore it is very important to find out possible factors that may influence the adoption of e-government services (Rehman & Esichaikul, 2011). The issue of trust, reliability, availability, status reporting and expediency are comparative advantages of e-government over traditional manual government operations (Akkaya et al., 2012). Findings in a research conducted by Akkaya et al. (2012) suggested that data protection/privacy is also one of the topmost motivations for the usage of e-government services.

Weaknesses of E-government Services

Not all citizens are highly knowledgeable about the overall use and operation of the e-government applications because of few technical add-ons. It will be rather too hasty for government to assume that a greater percentage of citizens are Internet

savvy, there are relatively huge IT skills gap amongst government employees as well. Secondly, in situations where usage of the application is not a problem, citizens may not be very knowledgeable about staying safe online, how not to expose private information to unauthorized personnel. These are some of the weaknesses of e-government. Security experts while designing applications for e-government must ensure that the security policies in place takes into account that e-government is dealing with not just the enlightened public but the unenlightened and uneducated as well. Little assumption should be made as regards the capacity of users, proactive security measures must be in place to protect citizens using the e-government platform to carry out their civic responsibilities (Shahintash et al., 2014).

In trying to find out factors that may give rise to breach of security within the e-government system, which could be classified to stem from both technical and human factors.

Human Factors

In the course of carrying out legitimate day-to-day functions of government utilizing computer applications, wrong values could be entered in the wrong fields, or sometimes the wrong files will be deleted or altered. Innocent mistakes are very prevalent, though often accepted as inevitable human errors that could be immediately corrected when identified. In information security, such innocent errors may result in security implications: a situation whereby e-government users pass on sensitive data to not very trusted websites; sometimes downloading misleading programs and imprudently submitting personal data to them. Azeez at al. (2012) stated in their paper titled “Threats to e-government implementation in the civil service, Nigeria as a case study” that there were inadequately qualified IT personnel in the federal civil service in Nigeria and the government was reluctant to train staff considering the huge financial implications. This lack of adequate training among users of e-government systems makes them not to observe strict security precautions: they sometimes unknowingly open network ports; most firewall

vulnerabilities are not checked therefore giving way to certain security breaches (Shahintash et al., 2014; Nkohkwo at al., 2013). Asogwa (2013) also supported the argument by saying that limited technical experience (shortage of skilled manpower) in ICT makes it difficult to handle those technical applications provided by e-government.

Technical Factors

In a study conducted by Asogwa (2013) amongst employees in federal government ministries in Nigeria about factors relating to technology and management of information within e-government services, members of staff stated that there were several unforeseen challenges experienced since the deployment of e-government in the ministry. They considered the change from manual to electronic to be too fast, making particular reference to the issue of storage devices; most of the respondents complained about the frequent manner with which storage devices are changed due to technological exigencies; and often times government is not very flexible to these changes. She argued that most African countries do not make adequate preparation for e-government adoption, therefore missing out vital requirements. This may also has reduced the eagerness for online solicitation of citizens' perception on critical policy issues of government. Technological factors include a selection of dedicated protective services such as tools used for encrypting and decrypting data, firewalls, and secure file systems, unique personal identity numbers, biometric devices and tokens. If usages of these devices are raised over a capacity limit, it may slow down the performance of the entire system protection, thereby making the execution system slow and also exposing the system to the vulnerabilities or more breaches. Ashaye et al. (2013) also demonstrated in his paper titled "e-Government implementation benefits, risks and barriers in developing countries: evidence from Nigeria" that service fragmentation and introduction of new technologies pose a risk to availability as the government is still over-dependent on foreign-based technical expertise. The response time to certain system failures may be too long in situations where local expertise may not be sufficient.

All security threats introduced by users of the Internet could have an effect on the security of e-government service infrastructure. Often times, government organisations interact with one another without any functional security prevention mechanism put in place (Ashaye et al., 2013).

It is very important to put in place security strategies to ensure that government establishments have optimal system performance and implement all-inclusive security defence mechanisms.

In spite of the level of security and privacy techniques implemented, there are some critical features that are still absent on some e-government websites, as demonstrated by the United Nations e-government development 2012 survey, which shows that only 20% of national e-government websites clearly specify existence of security characteristics on their sites. Europe leads with about 44% of nations that display signs of security on their websites, as compared to other continents (Shahintash et al., 2014).

United Nation's E-government Survey

The United Nations department of economic and social affairs (UNDESA) through its department for public administration and development management (DPADM) conducts and publishes the United Nations E-Government Survey every two years. It is a representation of comparative rankings of e-government development amongst member states of the United Nations. Through the rankings the performance of individual countries are placed on a comparative scale, the survey makes relevant information available to support top government decision-makers in determining their e-government programmes for development (United Department for Economic and Social Affairs, 2014).

Currently, the 193 United Nations member states do have national websites; however a high majority of them are still at rudimental or intermediate levels of e-government development, otherwise referred to as emerging and enhanced stages in the United Nations e-government maturity stages. Notwithstanding countries with very sophisticated technical prowess and highly skilled and resource

capabilities, it could still be very complex to progress to the higher levels that involves transactional and connected services, knowing that these stages usually need very robust data protection methods, and also very secure information sharing across government organisations (United Department for Economic and Social Affairs, 2014).

Table 3.1 shows the UN e-government rankings in the year 2012 of the top 20 most developed nations according to the UN e-government development index. The focus of the United Nations e-government assessment in this particular year was principally on the idea of service integration that utilizes inter-operability amongst all public services, functioning both practically and theoretically as a one-stop-shop portal, thus enhancing user experience and giving room for effective back-end service integration across governmental institutions while improving institutional measures. Based on the goal of developing e-government solutions to improve government service delivery and improve processes in government organisations, the rankings of 2012 contain an assessment of the development of e-government that centred on integrated services as well as user-centricity. Amongst the 20 top-ranking countries, 14 of the countries are in Europe and North America, 4 from Asia and 2 from Oceania, with none from Africa. The Republic of Korea ranked 1st followed by the Netherlands in 2nd position and the United Kingdom ranked 3rd above Denmark, the United States of America and France which ranked 4th, 5th and 6th. Sweden ranked 7th, Norway 8th, Finland 9th, Singapore 10th, Canada 11th, Austria 12th, New Zealand 13th, Liechtenstein 14th, Switzerland 15th, Israel 16th, Germany 17th, Japan 18th, Luxembourg 19th and Estonia is the 20th top-ranking country in the year 2012. The table shows the highest country's e-government development index (EGDI) for that year as 0.9283 and the 20th as 0.7987 respectively.

Table 3:3 UN survey ranking of world e-government leaders for the year 2012

Rank	Country	e-government development index
1	Republic of Korea	0.9283
2	Netherlands	0.9125
3	United Kingdom	0.8960
4	Denmark	0.8889
5	United States of America	0.8687
6	France	0.8635
7	Sweden	0.8599
8	Norway	0.8593
9	Finland	0.8505
10	Singapore	0.8474
11	Canada	0.8430
12	Australia	0.8390
13	New Zealand	0.8381
14	Liechtenstein	0.8264
15	Switzerland	0.8134
16	Israel	0.8100
17	Germany	0.8079
18	Japan	0.8019
19	Luxembourg	0.8014
20	Estonia	0.7987

Table 3.2 shows e-government development in the largest populated countries according to the UN e-government ranking in the 2012. The countries shown are those countries whose population were above one hundred million people within the period, their EGDI in 2010/2012 and also their rankings for 2010/1012, respectively. China with an estimated population of 1,341,000,000 people ranked 72 in 2010 and 78 in 2012; India with an estimated population of 1,225,000,000 people ranked 199 in 2010 and 125 in 2012; the USA with an estimated population

of 310,000,000 ranked 2nd in 2010 and 5th in 2012; Indonesia with an estimated population of 240,000,000 ranked 109 in 2010 and 97 in 2012; Brazil with an estimated population of 195,000,000 ranked 61 in 2010 and 59 in 2012; Pakistan with an estimated population of 174,000,000 ranked 146 in 2010 and 156 in 2012; Nigeria with an estimated population of 158,000,000 ranked 150 in 2010 and 162 in 2012; Bangladesh with an estimated population of 149,000,000 ranked 134 in 2010 and 150 in 2012; the Russian Federation with an estimated population of 143,000,000 ranked 59 in 2010 and 27 in 2012; Japan with an estimated population of 127,000,000 ranked 17 in 2010 and 18 in 2012; Mexico with an estimated population of 113,000,000 ranked 56 in 2010 and still maintained the 56th position in 2012. Amongst the most populated developed countries, the USA is shown to be the country with the highest ranking in the years reported in the table. The USA ranked 2nd in 2010 and 5th in 2012, with Japan ranking a distant 17th in 2010 and 18th in 2012, making only the USA and Japan rank amongst the top 20 world e-government leaders.

Table 3:4 E-government developments in the largest populated countries 2012

	E-government development index		**World e-government development ranking**		**Population (millions)**
Country	**2012**	**2010**	**2012**	**2010**	
China	0.5359	0.4700	78	72	1,341
India	0.3829	0.3567	125	199	1,225
USA	0.8687	0.8510	5	2	310
Indonesia	0.4949	0.4026	97	109	240
Brazil	0.6167	0.5006	59	61	195
Pakistan	0.2823	0.2755	156	146	174
Nigeria	**0.2676**	**0.2687**	**162**	**150**	**158**
Bangladesh	0.2991	0.3028	150	134	149
Russian Federation	0.7345	0.5136	27	59	143
Japan	0.8019	0.7152	18	17	127
Mexico	0.6240	0.5150	55	56	113

Table 3.3 shows the Top 20 leading African Countries E-government Development Index EGDI for 2014; it also shows a description of the income level of the respective countries. It shows the rankings of the year 2012 and 2014 for comparative purposes, providing a column that shows the difference or progress or decline between 2012 and 2014. Tunisia with an upper middle income level ranked 103 in 2012, it moved 28 points upwards to rank 75 in 2014; Mauritius with an upper middle income level ranked 93 in 2012, it moved 17 points upwards to 76 in 2014; Egypt with a lower middle income level ranked 107 in 2012 but moved 27 points upwards from 107 in 2012 to rank 80 in 2014; Seychelles with an upper middle income level ranked 84 in 2012 but moved 3 points upward to rank 81 in 2014; Morocco with a lower middle income level ranked 120 in 2012 but moved 38 points upwards to rank 82 in 2014; South Africa with an upper middle income level ranked 101 in 2012 but moved 8 points to rank 93 in 2014; Botswana with an upper middle income level ranked 121in 2012 but moved 9 points to rank 112 in 2014; Namibia with an upper middle income level ranked 123 in 2012 but moved 6 points upwards to rank 117 in 2014; Kenya with a low income level ranked 119 in 2012 but maintained the same ranking of 119 in 2014; Libya with an upper middle income level ranked 191 in 2012 but moved 70 points upwards to rank 121 in 2014; Ghana with a low middle income level ranked 145 in 2012 but moved 22 points upward to rank 123 in 2014; Rwanda a low income level ranked 140 in 2012 but moved 15 points upwards to rank 125 in 2014; Zimbabwe with a low income level ranked 133 in 2012 but moved 7 points upwards to rank 126 in 2014; Cape Verde with a lower middle income level ranked 118 in 2012 but moved 9 points downwards to rank 127 in 2014; Gabon with a lower middle income level ranked 129 in 2012 but moved 2 points downwards to rank 131 in 2014; Algeria with a lower middle income level ranked 132 in 2012 but moved 4 points downwards to rank 136 in 2014; Swaziland with a lower middle income level ranked 144 in 2012 but moved 6 points upwards to rank 138 in 2014; Angola with a upper middle income level ranked 142 in 2012 but moved 2 points upwards to rank 140 in 2014; Nigeria with a lower middle income level ranked 162 in 2012 but moved 21 points upwards to rank 141 in 2014

and Cameroon with a lower middle income level ranked 147 in 2012 but moved 3 points upwards to rank 144 in 2014. It is apparent that Libya made a remarkable development within the period, leaping from a distant 191 to 121 in two years. Nigeria, which is the focus of this research, moved 21 points upwards, which was commendable but it is still considered rather slow in its development.

Table 3:5 Top 20 leading African Countries EGDI 2014

Country	Level of Income	EGDI	2014 Rank	2012 Rank	Change in Rank
High EGDI					
Tunisia	Upper Middle	0.5390	75	103	28 ↑
Mauritius	Upper Middle	0.5338	76	93	17 ↑
Egypt	Lower Middle	0.5129	80	107	27 ↑
Seychelles	Upper Middle	0.5113	81	84	3 ↑
Morocco	Lower Middle	0.5060	82	120	38 ↑
Middle EGDI					
South Africa	Upper Middle	0.4869	93	101	8 ↑
Botswana	Upper Middle	0.4198	112	121	9 ↑
Namibia	Upper Middle	0.3880	117	123	6 ↑
Kenya	Low	0.3805	119	119	-
Libya	Upper Middle	0.3753	121	191	70 ↑
Ghana	Lower Middle	0.3735	123	145	22 ↑
Rwanda	Low	0.3589	125	140	15 ↑
Zimbabwe	Low	0.3585	126	133	7 ↑
Cape Verde	Lower Middle	0.3551	127	118	9 ↓
Gabon	Upper Middle	0.3294	131	129	2 ↓
Algeria	Upper Middle	0.3106	136	132	4 ↓
Swaziland	Lower Middle	0.3056	138	144	6 ↑
Angola	Upper Middle	0.2970	140	142	2 ↑
Nigeria	**Lower Middle**	**0.2929**	**141**	**162**	**21** ↑
Cameroon	Lower Middle	0.2782	144	147	3 ↑

Table 3.4 is a representation of leaders of e-government by region in the year 2014, starting alphabetically from Africa, which has Tunisia and Mauritius as the leaders of e-government in the continent; the Americas have the USA and Canada as the leaders of e-government the region; in Asia, it is South Korea and Singapore that are the leaders of e-government; in Europe, France and the Netherlands are the leaders of e-government, while in Oceania it is Australia and New Zealand that are the leaders.

Table 3:6 Leaders of e-government by region 2014

World e-government leaders		**Regional Leaders**	
South Korea		AFRICA	Tunisia
Australia			Mauritius
Singapore		AMERICAS	United States of America
France			Canada
Netherlands		ASIA	South Korea
Japan			Singapore
United States of America		EUROPE	France
United Kingdom			Netherlands
New Zealand		OCEANIA	Australia
			New Zealand

South Korea did retain the highest position in 2014 through its sustained leadership and vision in the advancement of e-government. Singapore and Australia also improved significantly above their 2012 global rank. Accordingly, the 2014 survey demonstrates that Europe has consistently maintained the lead in the top regional E-government Development Index (EGDI), next to the Americas led by the United States of America, ranking seventh in the world; South Korea is also the leader of the Asia region; Australia leads in the Oceania region; while Tunisia is the leader of the African region ranking 75th globally.

Consequent upon the data presented in tables 3.1 to 3.4, this study investigates the reasons why some countries are slow in adopting e-government. What are the identifiable challenges and relevant implications of such challenges? An analysis of the survey conducted is presented in subsequent chapters.

Brief History of Nigeria

Nigeria is considered the most populous country in Africa, with much cultural diversity. It has over 250 ethnic groups with about 400 languages; the people in the northern part of the country are predominantly Muslims, while those in the southern part are predominantly Christians (Metz, 2002). The country gained her independence on the 1st October, 1960 from the British colony and became one of the founding members of the Commonwealth of Nations.

The country is divided into six geo-political zones namely: South-South, South-West, South-East, North-East, North-West and North-Central, while Abuja serves as the federal capital territory (FCT). Nigeria operates a presidential system of government with a bicameral legislative system, like the United States of America, the house of representatives is the lower house while the senate is the upper house both referred to as the national assembly. The presidential system consists of three tiers: the federal, the state and the local government (Teniola, 2014). Each tier of government has three arms: the executive, the legislative and the judiciary; they function independently so as to ensure the principle of checks and balances in the system (Teniola, 2014).

Nigeria's geographical location is on the Gulf of Guinea in Western Africa. It is positioned between Benin in the west and Cameroon in the east. To the north are Chad and Niger. With an area of 923,768 km² the country is almost four times the size of the United Kingdom. Nigeria has a population of 177.5 million people (UN estimate, 2014), making it Africa's most populous country. The capital city, Abuja, is located at the centre of the nation, while Lagos is the commercial hub and the primary port and largest city. English is the official language; some other prominent languages are Hausa, Yoruba, Ibo and Ibibio (NationsOnlineProject, 2015).

General literacy level is estimated at 61.3%; since the last report in the year 2010, an increase in general literacy level may increase computer literacy, which will encourage more citizens' interest towards e-government. In 2015, Nigeria was classified amongst the 20th largest economies in the world, based on a net worth of about US$500 billion and US$1 trillion nominal GDP purchasing power parity, making it the biggest economy in Africa (NationsOnlineProject, 2015). Figure 3:1 is the map of Nigeria showing all the 36 states and the federal capital territory at the centre, also showing the bordering countries.

Figure 3:2 Map of Nigeria

(NationsOnlineProject, 2015)

Level of Internet Penetration in Nigeria

According to the InternetLiveStatistics (2014) report on world Internet users by country as published January 2014, Nigeria ranked eighth in the world, a step ahead of the United Kingdom which was ranked ninth in the world.

Table 3:5 shows the global ranking of Nigeria from 2000 to 2014 in terms of Internet users, growth in Internet usage, new users per year, the country's estimated population per year, population change, percentage of Internet penetration of the population, the country's share of world population, as well as the country's share of the world's Internet users. Nigeria ranked top 20 for Internet users globally from 2000 to 2004; it maintained the top 20 position consistently for 4 consecutive years. In 2005, Nigeria was ranked 19th for top Internet user globally, reporting a 183% growth from about 1,749,138 users in the previous year to about 4,954,121 users; in 2006, it maintained the 19th position with 60% growth to 7,946,863 users; Internet users increased to 9,964,584 in 2007, which represents 25% increase from the previous year, yet maintaining the 19th position in the global ranking; in 2008, there was an upward movement by 4 points from 19 to 15 on the global ranking, representing a 141% increase to 23,981,608 users; from 2009 to 2011, Nigeria ranked 10th for global Internet users, remarkably, with user population of 31,076,204 in 2009, 38,329,867 in 2010 and 46,680,049 in 2011; in 2012, there was a 19% increase in user growth to 55,506,299, making the country rank 8th globally; in 2013, Nigeria maintained the 8th position, but with a user growth percentage increase of 16% to 67,101,452 users, and in 2014, Nigeria still maintained the 8th position globally, this time with a user population growth of 12% to 75,746,751 Internet users. The core reason for displaying this in table 3.5 is to make a comparison between Internet penetration and the e-government development index shown earlier in tables 3.2, 3.3, and 3.4, respectively.

Table 3:7 Statistics of Internet Usage in Nigeria from 2000 to 2014

Year (July1)	Internet Users	User Growth	New Users	Country Population	Population Change	Penetration% of pop. With Internet	Country's share of World population	Country's share of world Internet Users	Global Rank
2014	75,746,751	12%	8,645,299	177,475,986	2.63%	42.7%	2.4%	2.30%	8
2013	67,101,452	16%	9,365,590	172,816,512	2.70%	33.26%	2.42%	2.13%	8
2012	55,506,299	19%	8,826,250	168,833,776	2.83%	32.88%	2.38%	2.20%	8
2011	46,680,049	22%	8,350,181	164,192,925	2.81%	28.43%	2.35%	2.04%	10
2010	38,329,867	23%	7,253,663	159,707,780	2.78%	24.00%	2.31%	1.84%	10
2009	31,076,204	30%	7,094,603	155,381,020	2.76%	20.00%	2.27%	1.76%	10
2008	23,981,608	141%	14,017,018	151,208,080	2.73%	15.86%	2.24%	1.53%	15
2007	9,964,584	25%	2,017,720	147,187,353	2.70%	6.77%	2.21%	0.73%	19
2006	7,946,863	60%	2,992,743	143,314,909	2.67%	5.55%	2.27%	0.68%	19
2005	4,954,121	183%	3,204,983	139,585,891	2.64%	3.55%	2.14%	0.48%	19
2004	1,749,138	136%	1,008,744	135,999,250	2.60%	1.29%	2.11%	0.19%	20
2003	740,394	79%	326,278	132,550,146	2.57%	0.56%	2.08%	0.10%	20
2002	414,116	266%	300,836	129,224,641	2.56%	0.32%	2.06%	0.06%	20
2001	113,280	44%	34,540	126,004,994	2.55%	0.09%	2.03%	0.02%	20
2000	78,740	60%	29,563	122,876,727	2.54%	2.54%	2.01%	0.02%	20

Source: InternetLiveStatistics (2014)

The above data elaboration was presented by the International Telecommunication Union (ITU), United Nations Population Division, Internet & Mobile Association of India (IAMAI), and the World Bank.

E-government varies from one country to another. Governments all over the globe are at different stages of e-government preparedness and adoption, according to the UN e-government report on the different levels of e-readiness, with countries in Europe usually appearing in the top ranks (Ayanso et al., 2011).

To be e-ready, a country must have the required regulatory and institutional frameworks to provide a firm foundation for e-government transactions and making sure that citizens find it convenient to use the e-government services deployed. It is very apparent from the EGDI that Africa is still less developed in terms of e-government adoption (Ayanso et al., 2011).

The spread of the internet and the eventual development of e-government came with some potential dangers to information privacy. There has been a growth in online data theft, particularly user identities, and in most cases laws regulating cyber related crimes are absent or in the processes of legislation. The target of these criminals is unique identification numbers, like social security numbers, national insurance numbers, credit card details or PINs (Adedayo et al., 2013).

Nigeria was listed amongst twenty nations with the highest rate of internet penetration, stating that in the year 2011, Nigeria had over 45 million internet users, according to the online report, making the country 11th on the global rating of internet users next to France; Nigeria's internet penetration ratio was 26.5%. This high internet penetration, according to a report by Adedayo et al. (2013), "sparked a tremendous growth in online transactions. In just a year, the number of Internet users in Nigeria rose by 19%, to 55 million users in 2012" (Adedayo et al., 2013, p.625).

Aspects of the Implementation of E-Government Security Strategies in Both the Developed and Developing Countries

The plans and strategies to implement e-government in the developing nations of the world have always depended on the technique and practices put in place by the very established developed nations. In a bid to advance their nations in terms of efficient service delivery to the yearning public, developing countries most often hurriedly put together what could be described as online government service without an adequate strategy.

Nevertheless, because of significant disparity in several major part of e-government as it relates to social and technological applications in the developed and the developing nations, all the practices implemented in the advance countries may not be very practicable in the developing countries.

Chen et al. (2006) stated that in most developed countries, “some 20 to 25% of e-government initiatives are mostly never completed or dumped directly after commissioning, another 33% stop working partly because of failing to achieve set objectives, causing significant undesirable outcomes” in their publication titled “E-government Strategies in Developed and Developing Countries: An Implementation Framework and Case Study” (Chen et al., 2006, p.29).

The Need to be E-Ready

Government preparedness to implement e-services is referred to as e-readiness; this preparedness is based on technical, institutional, managerial, human resources components. The determination on the part of government to improve service delivery will give rise to this preparation, by making budgetary provisions available. To be e-ready has to do with ensuring there requisite legal and regulatory structures are in place to support e-government deployments and also to ensure that users are comfortable to carry out their transactions on e-government platforms (Darren, 2011).

E-Government Implementation in Nigeria

While e-government implementation is still on-going in Nigeria, it is not very easy to find any evidence of a literature suggesting that there is a strategy or framework put in place as a guide towards facilitating the easy adoption of e-government. There are some government websites that has been found to be delivering services online, but on the average it can be said that government online services are still at the emerging stages, only very handful are at the transactional stages (Darren, 2011).

Similar to several other African nations, there are some apparent problems that influence the operations of e-government in Nigeria.

Despite the high Internet usage in Nigeria as stated in Table 3.3, the United Nations world e-government ranking in the year 2014 reported Nigeria ranking a distant 141 in the world ranking (United Nations Department for Economic and Social Affairs, 2014). This clearly demonstrates the state of e-government development and adoption in Nigeria. Understanding the concepts of e-government and its governance practices around the world vis-à-vis the Nigerian situation; clarifications have to be provided to salient issues as regards it genuine preparedness. Analysis came to the fore that Nigeria faces a lot of infrastructure, social and human problems, which if not properly tackled, may make the foundation of e-government a very difficult task.

Reports have it that Nigeria is faced with huge infrastructural deficit, which may require a deliberate and concerted effort on the part of government to ensure the required infrastructures are put in place, otherwise there would be no foundation for the deployment of an e-government system. The situation no matter how daunting it may seem, there are viable way out, countries like Singapore were in a similar situation but presently they have recorded a success story in e-government to the benefit of the citizens. With globalization, only “electronic enabled” states may show relevance in international affairs both in commerce and politics (Dode, 2007).

Nigeria constituted an e-government project known as “National e-government Strategy” (NeGSt) to enhance the efficient delivery of public services through the utilization of relevant Information and Communication Technology tools. The aim was that an improved service delivery will engender more productivity that will foster rapid growth in the economy as well as national competitiveness. Unfortunately, the plans did not turn out according to the projections of the initiators of the scheme (Asogwa, 2013).

According to a study conducted by Asogwa (2013) to find out the challenges of e-government in Nigeria, he claimed that “about 77% of participants that responded says citizens privacy is a major reason why digital signatures and digital documents are inadmissible in many offices in Nigeria” (Asogwa, 2013, p.153). This response was probably looking at things from the perspective of corruption amongst government officials, it has been reported that most civil servants do not want the adoption of electronic services because it may expose illegitimate practices that existed within the system and thereby stopping the sources of illegitimate incomes. It has made the country to continue to transact most of its very sensitive businesses on the traditional paper based methods, making government very cumbersome. There have been several reported cases of missing files during movements of files from one office to the other, it is therefore very apparent that protection of user privacy and adequate measures to avoid the abuse of public functions remains an essential prerequisite for having a flourishing e-government. Thus, respondents in Nigeria observed that security and privacy of users is the utmost challenge to e-government (Asogwa, 2013).

E-Government Initiatives in Nigeria

According to the report of the United Nations Public Administration Network, Nigeria is ranked amongst the most populated countries in the world. During the ranking of top most developed countries in terms e-government, Nigeria did not feature in the list of top 10 leaders in Africa in e-government development.

It is therefore very challenging especially for the government through the Federal Ministry of Communication Technology, where the minister and other top functionaries are supposed to accelerate the adoption of e-government first within government to government transactions (United Nations Public Administration Network, 2013).

The National Information Technology Development Agency (NITDA) pioneered an e-government framework project in the year 2010 that was to lay the necessary structures for the development of a purposeful e-government policy through which the nation's government vision to rank among the top 20 developed nations by the year 2020 will be realised.

According to a publication by the Federal Ministry of Communication Technology, the ministry did set out an initiative which has to do with the classification of critical government services so as to deliver the services online through the government website.

By the year 2012, the government has given approval for the implementation of IT shared services and the institutionalization of the rank of Chief Technology Officer Cadre in the federal civil service. With responsibilities to bring efficiency into the budget processes for Ministries, Agencies and Departments' (MDAs) IT projects, to set up consultative or advisory services on e-government programmes within the MDAs, to stimulate local participation and foster a joint approach towards a sustainable content development.

In addition to the above, the Nigerian government created more initiatives to propel e-government penetration by using the Open Government/Open Data Initiative, which was aimed at increasing less sensitive government information online in compliance with the Freedom of Information Act 2011. The ministry collaborated with the World Bank through the Korean Trust Fund to build what was called the Open Government Partnership (OGP) Country Plan and Technology Roadmap for OGP. In the same year 2012 there was an ongoing effort aimed at deploying very integrated e-service as a response to citizens' agitation for improved

service delivery and make the administration more transparent and service oriented, inculcating services that involves the use of the new media to enhance citizen's engagement and foster effectiveness in governance (Federal Ministry of Communications, 2015).

The country is yet to get to the transactional level of e-government; majority of the government websites primarily contains government information and forms. It was apparent as at 2013 that Nigeria was gradually moving towards the transactional stage of e-government, particularly the Nigeria Immigration Service providing online visa and international passport applications. Developing to the transactional stage will come with many risks without a robust security framework which will be based on relevant laws and policies (Adedayo et al., 2013).

The establishment of NITDA in the year 2001 was basically to initiate strategic practices that will ensure competitive utilization of ICT infrastructures by the citizens and corporate organisations in the country.

The initiative however good intentioned they were couldn't accomplish the desired objectives because it lacked proper regulatory framework for best practices thereby allowing the system of cybercrime to fester without control (Adedayo et al., 2013). Most of the government websites were compromised and defaced and the hackers boasted by saying that the websites were not professionally secured that several back doors were left open. The ministry of foreign affairs that is saddled with the responsibility of administering the affairs of Nigeria embassies and high commissions abroad was among top departments of government that it website was tampered.

Several efforts has been put in place to adopt full scale e-government, but there are limited evidence of a study that shows that a comprehensive construct or framework for the development of a secure e-government is in place so that it will be referenced during implementation, therefore this research is essential. Recently, the national security adviser to the Nigeria President reported that: "The 2014 annual report of the Nigeria Deposit Insurance Corporation (NDIC), found that,

between the year 2013 and 2014, fraud on e-payment platforms of the Nigerian banking sector increased by 183 per cent. He further said that, a report published in 2014 by the Centre for Strategic and International Studies, UK, estimated the annual cost of cybercrime to Nigeria at about 0.08 per cent of the nation's GDP, which represents about N127 billion Naira" (Iroegbu, 2016, p.8). He further cited that "global tracking of cyber-attacks indicate that Nigeria is among countries with high cases of software piracy, intellectual property theft and malware attacks" (Iroegbu, 2016, p.8).

Summary

The conceptual framework gave a vivid overview of initial concepts, opinions and existing reports that characterise the implementation of e-government services. It discussed issues that led to the conceptualization of the topic of the study. Potential factors that could influence the adoption of e-government and those that could impede the use of e-government were vital to be examined. A closer look at the United Nations e-government survey that ranks countries' performances on a comparative scale indicated that Nigeria has not fared well amongst its contemporaries despite its huge economic posture in the African region.

In the 2012 United Nations survey of world leaders in e-government, Nigeria was not among the top 100, which had South Korea as the first, the Netherlands second and the United Kingdom third, while Nigeria ranked a distant 162. In the 2014 survey, Nigeria ranked 141 while South Korea maintained the lead. It was however commendable that between 2012 and 2014, Nigeria climbed 21 points upwards from 162 in 2012 to 141 in 2014, as shown in Table 3:3. The development was however considered very slow when compared to Libya, which moved 70 points upward from 191 in 2012 to 121 in 2014, Morocco moved 38 points upwards, and Tunisia moved 28 points upwards to rank 75th in the world and first in Africa, as indicated in table 3:3.

Hence, the research questions, what is responsible for the slow development of e-government in the developing countries? What are the contending issues, what is the possible way forward?

Methodology

Introduction

To accomplish the aim and objectives in a valid research manner, defining a clear and appropriate research methodology is essential. This chapter presents a systematic, well-structured and logical way in which this research problem was carried out, the procedures by which the research was conducted, describing and explaining or even predicting phenomena, according to Rajasekar et al. (1994). This includes the underlying research methods chosen, questions asked, data collected and techniques used for data analysis. The criteria for identifying the relevant questions that will be asked and the reasons for choosing those questions; also to illustrate the methods that were used to provide answers to the research questions and also describe practical steps involved in the implementation of the strategy. This chapter discusses plans and procedures for analysing data collected while also demonstrating how to validate and check for how reliable the data sets are.

Research Philosophy

There are different methods of carrying out a research, the choice of a particular approach or method could be consequent upon the philosophy behind the research. In discussing philosophy of research, some terms needs to be explained. What is epistemology, epistemology originates from a Greek word known as *epistêmê*, meaning knowledge; it stands for the philosophy of knowledge or the way we came to know what we know (Krauss & Putra, 2005). Just like methodology and ontology, epistemology has to do with realism, it deals with the way we became aware of reality while methodology finds out practical steps involved in acquiring knowledge about a thing.

Epistemology tends to find out the correlation between what is known and the one that knows it. How we got to know about the things we know? What knowledge is deemed to be?

Interpretivism

Interpretivists are of the notion that reality can only be understood by way of interpreting a phenomenon subjectively. Studying a phenomenon in its nature state is central to the philosophy of interpretivism, while acknowledging the fact that scientists may probably always have some influence over what is it they are studying (Saunders et al., 2009). They are also of the opinion that there could be several understanding of the term reality, nevertheless these understanding are inherent components of the methodical knowledge been pursued. Interpretivists do not subscribe to the idea of a single reality, believing any notion of "reality" to be constructed by any individual or groups, so there are multiple realities in the world, and different research approaches are likely to lead to different research outcomes (Oates, 2006). Interpretivists would not always expect convergence in data they generate data using a process known as triangulation.

Positivism

The positivist presumption is that any object under investigation is not totally dependent on the views of the researcher; that fact is revealed and confirmed through clear process of observing of a phenomenon. It subscribes to the idea of single "truth" or "reality" and would expect multiple lines of attack to lead a consistent set of findings (Oates, 2006).

Alternatively, the naturalist or constructivist's perspective is that knowledge is verified judging from the meanings ascribed to the phenomena under investigation; researchers relate with the phenomenon under investigation to find facts; during investigation the views of the researcher may change about subject matter; and understanding depends on time and the context (Lin, 1998; Creswell, 2003).

Pragmatism

Saunders et al. (2009) asked a question in trying to justify the concept of pragmatism: it sought to ask if we must all accept a particular position on any subject matter? Even though we consider accepting the assertion by Guba et al.

(1994) which states that every question about methodology are less important to questions relating to epistemology or ontology. It is acceptable to think that it is rather impractical to make a choice between two or combining two opposing views.

Pragmatism considers that the most significant element of ontology and epistemology that can be adopted in a study is the research question; a method of deriving answers in a particular circumstance may be more apt than another. Furthermore, if a given research question is clear about the adoption of either the positivist or the interpretivist philosophical approach; it may confirm the pragmatist's posture that it is absolutely feasible to adopt different methods.

Therefore it is very possible and right to use both quantitative and qualitative methods known as mixed method in a single research. Tashakkori and Teddlie (1998) argued that the pragmatic approach is naturally more attractive, mainly due to the fact that the researcher is not engaged in arguments of the theory of the difference between reality and truth. Researchers are at liberty to consider studying whatsoever interest them and may bring some value to them, study in any kind of way that is suitable and come up with research outcomes that may stimulate positive results (Tashakkori and Teddlie 1998).

One of the first critical tasks in a research is to come to a decision on which approach is most suitable to identify the right solution from where one can derive adequate conclusion as it relates to the phenomenon been studied (Patton, 1990). The choice of a very suitable research approach in the field of information systems and other associated phenomena is always a difficult choice to make, due to the fact that information systems offers researchers several approaches or strategies without limiting them to just one method (Saunders et al., 2009).

Choosing a Research Method

Quantitative Research

In general, quantitative research has to do with the positivist or postpositivist theory. It typically involves the collection and conversion of data into numerical forms so as to make or draw statistical inferences (Alzheimer Europe, 2009).

In quantitative research, we must observe the principle of objectivity. Therefore, researchers are expected to be very careful so that his personality preference, actions or feelings will not influence the outcome of study in a certain way. Researchers must also critically observe their techniques and results to avoid likely bias.

Qualitative Research

Basically qualitative research methods could be related to the social constructivist theory that lays emphasis on the publicly constructed characteristic of reality. It involves taking records, making analyses and determining the importance and impact of the behavioural patterns, experiences, conflicting beliefs as well as emotional reactions of human beings. Researchers seem to show interest in understanding the complex nature human experiences (Guba & Lincoln, 1994).

Qualitative researchers are more predisposed to using an inductive approach which indicates that they may build their hypothesis on the foundation of the data that they got from the field. This process has to do with going from the particular to the universal and often referred to as the bottom-up approach.

When carrying out a research, it is important for the researcher to apply methods that will make participants to have a positive degree of independence and allow for spontaneity rather than persuading them to choose among options that have been fixed which probably may not be accurate or suitable to participant's point of view or line of thought. Participants also need conditions that guarantee freedom

of expression that is why sometimes data collection is conducted in a somewhat informal atmosphere.

In qualitative research, participants are mostly fewer than in quantitative research maybe because methods like interviewing takes more time and effort to complete necessary steps to come up with accurate statistical report for analysis.

Mixed Methods

The idea of combining different methods possibly started in 1959, at what time "Campbell and Fiske employed multiple methods to examine the validity of psychological traits, as they encouraged other researchers to use this 'multi method matrix' to examine multiple approaches to data collection in a study" (Creswell, 2003, p.15). This encouraged more researchers to mix methods, and almost immediately approaches related with field methods like interviewing and observing were carried out in combination with conventional surveys (Creswell, 2003). Taking cognisance of the fact that all methods have their constraints, it was considered that potential limitations inherent in a particular method could be augmented or deactivated accordingly in another method (Creswell, 2003).

To find a way of converging data sources across quantitative and qualitative methods is known as triangulation. The first idea of triangulation came along with several new grounds for combining various types of data, one technique can be entwined within another technique which may provide clues to other different analysis unit within the mixed methods approach (Bazeley, 2004).

Mixed methods are intrinsically not more or less suitable compared to particular methods of research. Generally, we may confirm validity from the suitability, meticulousness and the efficient way with which these methods are applicable and the precision observed in the measurement of facts rather than from the process of applying strict rules that must be adhered to (Bazeley, 2004). The researcher occasionally collects data that are open-ended with a principal objective of developing ideas from the data.

Since the pragmatic approach has to do with employing the methods that seems most suitable to the research problem and not entangled in the philosophical discuss on which approach is the best. Pragmatism affords the researcher the liberty to employ from alternative techniques, approaches, processes and methods usually related with either quantitative or qualitative research. It is apparent that all methods have its boundaries and that the alternative approaches are of complementary consequences to each other. Different methods could be used at a particular instance or utilizing one after the other.

In this study, the researcher started with a face-to-face interview with several participants, after which the outcome of the interview was utilized to develop questionnaires to be used in assessing citizen's opinions so that a statistical report can be obtained and analysed.

Due to the fact that every researcher reserves the right to select an appropriate method from a variety of methods based on the level of information required. This research required different approaches at different times; therefore the pragmatic approach was most appropriate.

Data Collection Techniques

Questionnaires

A questionnaire is a general method for collecting data whereby individuals are required to provide answers to a given set of questions in the same way that each person is asked to respond to the same set of questions in a prearranged order (Saunders et al., 2009). One of the advantages of a questionnaire is that the researcher can get so many responses, particularly from those who may not be able to grant interviews. Participants are not constrained to provide answers on the spot like in the case of an interview, but at liberty to think over it and return the questionnaire at a more convenient time though within the timeframe of the study.

The participants are not influenced by the presence of the researcher, although a number of people could tend to give responses that they consider to be socially

satisfactory. Participants are advised to provide honest answers so that researchers do not publish false report of a situation (Dillman, 2011).

Questionnaires may be distributed and managed in several ways, it could be via email, Internet links, personal distribution of hard copies at conferences and distribution at public places, e.g. post offices, campus lounge and so on.

The other special significance of personal distribution of the questionnaire is that there are people with disabilities or difficulties in reading or writing, therefore the presence of the researcher will help to assist in recording responses in areas where there may be such difficulty (Dillman, 2011).

Interviews

Interviews are classified as one of the most common ways of data collection qualitatively. The various strategies used in conducting qualitative interviews available in research came from different disciplines or viewpoints which have resulted into a broad distinction amongst interview approaches (DiCicco-Bloom & Crabtree, 2006).

Interviews are typically administered in person, it could be through physical one-on-one conversation or via telephone/online video conferencing (Lee, 1991; Guba & Lincoln, 1994; Lincoln, 2005).

A formal or informal approach can be adopted in administering an interview by the researcher, it could be done in such a way that the interviewee is allowed to discuss the topic generally with the interviewer so that he can take note of relevant points or the interviewee will have to respond to itemised pre-arranged number of questions (Denzin & Lincoln, 2005).

If you want the interviewee to speak generally on the topic while the interviewer will direct the discussion appropriately to make sure the salient points are covered, a semi-structured approach will be the best approach to use.

Sometimes researchers get distracted by taking records of conversations during an interview it is therefore recommended that permission should be sought to use a

voice recorder for the purpose while the interviewer concentrate on the questions and answer check-list and so he can take note of gestures made by the interviewee as they are also important (DiCicco-Bloom & Crabtree, 2006).

The methodology adopted by this research constitutes a combination of methods and processes (mixed method), each of which was considered to be most suitable for the particular research stage and task. By and large, however, the definition of problem statements and research questions throughout this research are all based on personal experience as well as critical analyses of relevant literature.

For the first research contribution, which deals with the examination of issues responsible for the slow adoption of e-government in developing countries using Nigeria as a case study, research was carried out by initially going through relevant literature; looking out for possible work done in this area, interviewing citizens and stakeholders in Nigeria, conducting survey using questionnaires in Nigeria. The second contribution was the advancement of a strategic framework for e-government security as a guideline for e-government implementation; the necessary literature was examined and the framework designed to address the key problems identified or envisaged. The creation of the framework was also guided by a standardized development model to support its structure and processes.

With appreciation of the scope and limitations, the research focus then shifted to a more controllable research problem within the framework's context. This problem was drawn from the analysis of a recognised situation and then backed up by available literature.

Techniques and Procedures for Data Collection

Sampling Method

In line with the objectives of this research as well as the concerns to be examined, it could have been better if a greater percentage of stakeholders in e-government participated in the interview. Nevertheless, because of limitation of time and resource as regards this research, a possible set of participants were selected.

Saunders et al. (2007) assert that a non-probabilistic sample is most often used when adopting a case study strategy. A non-probability sampling, according to Oppenheim (2000), "is a sample by which the probability of a person being selected from the total population is not known" (Oppenheim, 2000, p.233).

Primary Data Collection

While the data collected may possibly be analysed by employing quantitative means, it was stated by Jackson et al. (2008) that researchers may decide to gather either primary or secondary data as the case may be, both methods have its merits and demerits. When a researcher goes to the field to gather his own set of data, there exists a measure of control over every data obtained from the respondents. It also gives the researcher some level of assurance that the collected data will serve the research objectives.

Interview Aim

To get subjective views of citizens and policy makers in Nigeria, so as to correlate relevant data as to the current e-government developmental efforts, benefits as well as challenges for the purposes of proposing a bespoke solution.

Interview Questions and Target Participants

The interviews were set out to achieve a strategic purpose. The interview questions were set out to be open-ended; the interviews were carried out in Nigeria after the development of the objectives of this research. The purpose of this interview was to first of all assess the interviewees' perception of the strength of e-government over the traditional way of interacting with government. This was aimed at finding out the views of the people regarding the deployment of full scale e-government in Nigeria, and utilising it as a new tool for processing government operations.

Sample

To get a broad view, the interview during this period took place in the Federal Capital Territory, which houses the federal government ministries, agencies and

departments; Lagos, the commercial hub of Nigeria; and Port Harcourt, the city that hosts the multinational oil and gas companies due to a large deposit of oil mineral resources in the region. These three areas are where most pilot schemes start from, for example, when the federal government of Nigeria through the central bank started the cashless policy initiative, it started in Lagos before integrating other parts of the country (Yaqub et al., 2013).

The questions set out to validate the supposition that online transactions are much preferable to manual transactions in terms of convenience, speed and comfort.

The research set out to find out what where the possible causes of the slow adoption of e-government in Nigeria. Is it the lack of adequate information technology infrastructure, low computer literacy levels, lack of government commitment to e-government policies, concerns over security and privacy, lack of adequate manpower to man the IT infrastructure, as well the issues of legal and regulatory frameworks in the country.

The interviews were conducted in Nigeria through convenient sampling amongst relevant stakeholders in the information technology sectors: among the key interviewees were the Director of ICT, Federal Ministry of Communication Technology, Abuja; Legal Officer National Information Technology Development Agency (NITDA); Director General Osun State Information Communication Technology Agency; Head of IT and members of staff at Galaxy Backbone Limited (implementers of e-government Initiative of the Federal Government); members of staff of the Federal Ministry of Communications Technology; members of Computer Professionals of Nigeria (CPN); private sector IT consultants; students; civil servants; as well as citizens.

Interview Process

Some of the interviews were conducted face to face formally in their offices, while others took place at the venue of the annual e-Nigeria conference from the 5th to 7th December, 2013 in Abuja. The interviews lasted between 30 to 40 minutes. The

interview was recorded with a voice recorder and notes were taken which were later transcribed (see appendix I). The transcribed data were analysed using the six steps of 'Thematic Analyses' by Braun and Clarke (2006). Based on existing study a priori codes were developed to aid and allow for flexibility for codes to emerge from the transcripts.

The interview focus was to examine the assertion that threats to security and privacy are the key factors responsible for the slow pace of e-government adoption in Nigeria, considering that information security involves both technical and non-technical requirements. All interviews were conducted face to face. Before every interview, appointments were scheduled mostly through referral or direct booking, sometimes through designated officials. The researcher gave a summary of what the study was about and the significant role the interviewee would contribute. Before conducting any of the interviews, the researcher handed a covering letter to the interviewee that contained a brief profile, providing relevant details including: the research institution, country and a brief abstract and what the research set out to achieve.

The letter also guaranteed that all data collected will be in the university repository but will remain confidential data, and the interviewees are basically always anonymous.

Analysis

Phase 1 Transcription of Verbal Data

In this phase, the data collected (voice recording and notes) were transcribed verbatim into text, taking cues of nonverbal behaviours where necessary. This process is crucial as the quality of the transcription may impact on the outcome of the data analysis. The process further enhanced the researcher's familiarization and understanding of the data, which provided the opportunity to identify patterns and meanings in the data. See a copy of the interview transcript in appendix I.

Phase 2 Generating Initial Codes

This phase involved the creation of initial codes from the data; codes here mean the identification of semantic contents of the data that are of interest based on the focus of this research. Ensuring identification of every meaningful sentence or phrase in the raw data components, these codes were generated manually by using coloured highlighters to indicate potential patterns within segments of the data (see appendix II).

Phase 3 Searching for Themes

This phase started after all the data have been initially collated and coded, and a list of the codes identified across the data. This phase redirects the analysis by sorting the different codes into potential themes, then collating relevant coded data extracts within the noted themes. In sorting the different codes into themes, it is vital to use a visual representation such as tables or mind maps. In this study, a mind map was used, as shown in Figure 4.1.

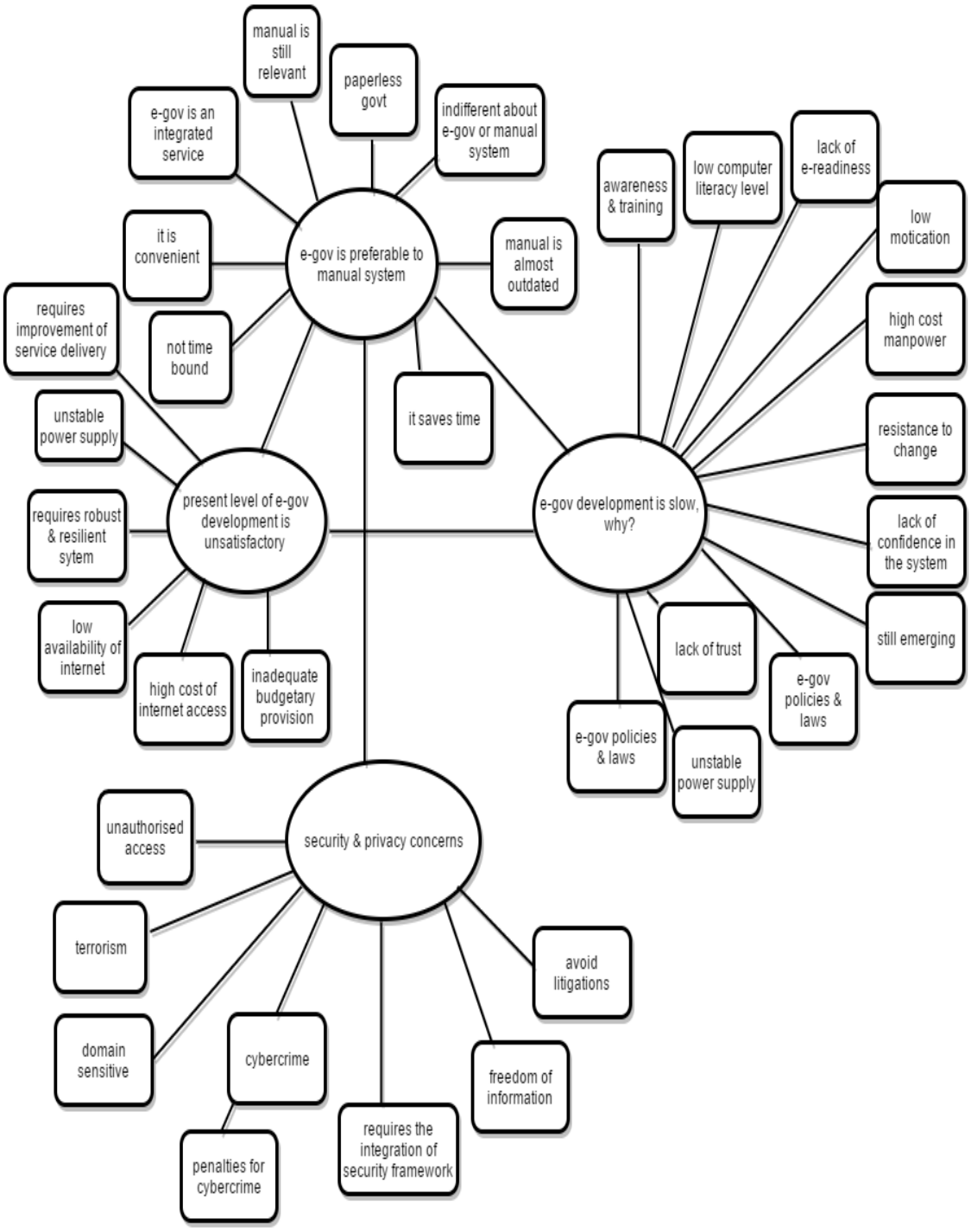


Figure 4:3 Initial Codes Sorted into Themes

Phase 4 Reviewing Themes

Phase 4 starts after a set of main themes have been made; it is about refining these already identified themes. At this time, it would have become apparent that some main themes were not eligible to be regarded as themes, e.g. situations where there is no sufficient data to back them up or the data extracted are too varied in meaning.

In some cases, themes that are similar in meaning collapse into each other to form one theme, while some others were broken down into two different themes. In as much as data within themes must be coherent, there must be clear distinctions between them (Braun & Clarke, 2006).

In this analysis, reviewing and refining the themes involves two stages: the first stage is to review the coded data extracts and involves reading the whole collated extracts for each theme to check if their patterns show some coherence. If they do, then continue to check main theme for coherence, wherever a theme does not actually fit rightfully then it requires re-working to find a place where it properly fits into the existing theme otherwise it will be discarded. A similar process is repeated at the second stage; here I tried to find how valid individual themes are in relation to the entire data set. Also, to verify the main thematic map is reflective of the true meaning expressed in the data. The process of coding and refining codes may continue forever; it is therefore important to realize when the refinements are no longer adding any significant changes, and then it time to stop and look out for the essential meaning based on the research questions. The result of the process of reviewing and refining of the themes is shown in the thematic map presented in Figure 4.2.

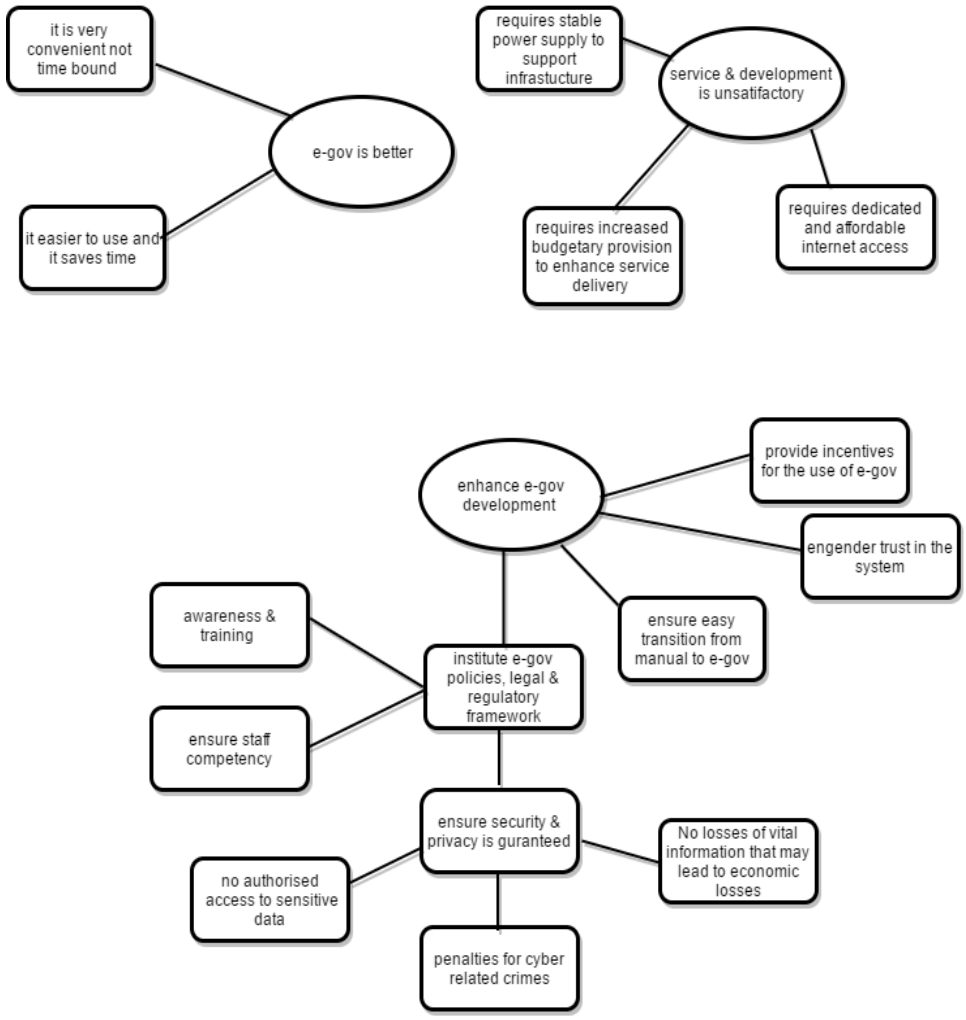


Figure 4:4 Refined Themes

Phase 5 Defining and Naming Themes

This phase is to further review and define the themes to be presented for analysis; it requires the identification of the essence of respective themes and to determine the specific aspects of the data each theme represents. I also had to consider if a theme contains sub-themes: sub-themes are primarily themes inside a theme; they could be useful in providing foundation to other complex themes and to

display different hierarchy of meaning in the data set. At the end of the analysis, two main themes and six sub-themes emerged; the main themes are e-government adoption and e-government survivability. The sub-themes are: political will, citizens training and awareness, affordable and uninterrupted access, information security laws and policies, e-government security framework, as well as trust in e-government services. The thematic diagram can be found in Figure 4.3.

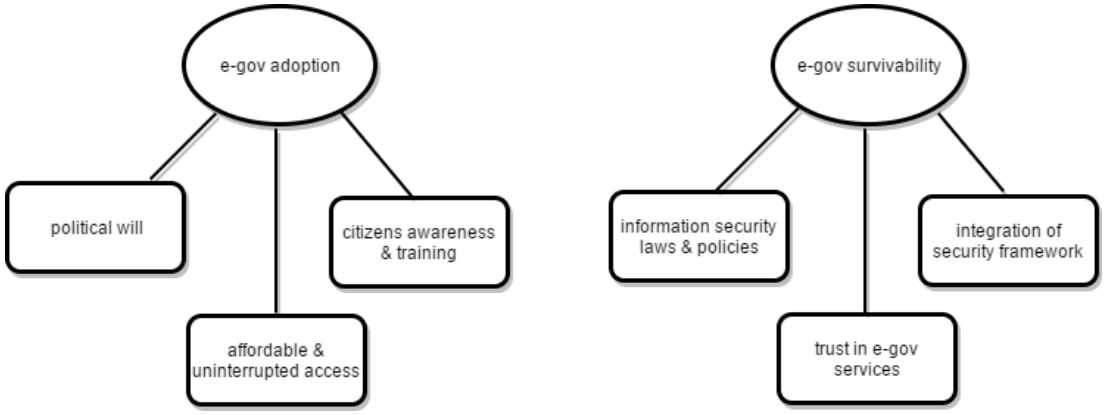


Figure 4:5 Final Main Themes and Sub-Themes

Phase 6 Findings from the Interviews

The qualitative data revealed that participants preferred the use of e-government transactions to the traditional ways of interacting with the government. They considered e-government to be more convenient to use as one could access services from different locations, not restricted by time. Hence, it is described as very effective and time saving, as citizens do not necessarily have to travel to a physical location just to fill out a form when it can be done online in a few minutes, as stated by one of the respondents.

> *"I will say yes, the reason been that e-government makes it easier for transactions to be completed faster than going physically to offices to carry out a particular transaction. It reduces the stress of travelling to different locations just to carry out a simple task, therefore doing it online is better." – Respondent 1*

Irrespective of the numerous advantages inherent in e-government services, participants considered its adoption in Nigeria as unsatisfactory and advocated for urgent measures to improve upon the present situation. They attributed the situation to the unstable power supply, low availability of Internet, high cost of broadband access, and generally a lack of robust and resilient e-government infrastructure. It was established that e-government in the country was still at the emerging levels, though some agencies have developed their e-government to a transactional level; but the level of adoption is still considered slow. A respondent presented his observation thus:

> *"Internet doesn't work optimally, secondly internet is still not very affordable, and government has to ensure that there is broadband penetration in the country. A situation whereby services are deployed online and it cost so much to access the service is already a great challenge to e-government adoption. Another factor is awareness, the people seem not be well aware of the usage of e-government, I also think the dwindling economic situation in Nigeria makes government not to be able to keep up with maintenance of e-government applications because the government has to import some facilities for e-government which requires foreign exchange. The Nigerian government doesn't have an adequate budget for e-government development." – Respondent 2*

Several reasons were given as possible factors responsible for the slow pace of e-government adoption in Nigeria: lack of e-government policies and regulations were identified amongst the main issues; at the time this data was collected in 2013, there were no laws against cyber related crimes, therefore citizens were sceptical about carrying out transactions online in an era where there were heightened concerns over cyber security and privacy. One of the respondents stated thus:

> *"Up till this moment there are no legal or regulatory framework for secure online transaction, citizens in my opinion may not have confidence to divulge their sensitive details on insecure government websites, particularly when they are aware that there are no defined penalties for cases related to online crimes." – Respondent 3*

Respondents considered citizens' lack of trust in the system as partly due to inadequate awareness and training or low literacy levels. Another factor was citizens' overall resistance to change; people were very reluctant to abandon the norm and adopt new technology. Bribery and corruption in the system was another factor. Citizens, particularly government officials that were benefitting from the proceeds of corruption did not want to encourage the adoption of e-government because it was going to make it difficult for people to circumvent the system to commit fraud. Therefore powerful forces in the system resisted the adoption of e-government.

> *"Several things, a lot of bribery and corruption take place in the traditional system, people are aware that if the electronic systems are fully functional, it may be difficult for them to continue their unwholesome practices, some other concerns are the government may not be able to pay professionals that will operate the hi-tech system used to deliver e-services, therefore the e-government system that government will provide may not be resilient." – Respondent 4*

The findings of these interviews gave a momentous review of the conceptual framework of the research, leading to the identification of crucial issues. The choice of a semi-structured interview was made because the researcher required definite answers to the questions prepared beforehand, which was to realistically confirm the initial concepts: to know how those initial perceptions influence e-government adoption generally by government, citizens and businesses. To improve the level of e-government adoption, issues of security and privacy have to be addressed.

Questionnaire Survey

As indicated earlier, the research utilized responses from the respondents in the interview to develop a questionnaire to citizens to enable the recording of quantitative data. Owing to the objectives of this research which is to obtain the opinions of policy makers, service providers and the general public. Hence, there was deliberate reduction of technical jargons where necessary in order to reduce ambiguity among participants.

Those that responded to the questionnaires were ICT top decision-makers in the public sectors, ICT top decision-makers in the private sectors, ICT personnel in the public sectors, ICT personnel in the private sectors, and members of academia as well as general end users. There were ten questions in the questionnaire though not all the analyses are reported, the ones that are reported are those considered very relevant at this level of the study and are presented in the following section.

Survey Analysis

The following sections provide details of responses from participants in the survey, over 250 questionnaires were distributed, through emails, Facebook Messenger and physical distribution at the annual e-Nigeria conference. Though out of the over 250 questionnaires that were distributed, only 160 responses were received, none amongst the ones received was rejected during the analysis. The second round of data collection was to validate the framework that was designed through expert opinion; experts in the industry were given an opportunity to evaluate the framework and give comments according to prescribed questions to enable easy analysis and reporting. These experts were chosen from amongst attendees of the e-Nigeria conference, an annual conference organised by the National Information Technology Development Agency for IT professionals and policy makers in the IT and Communications sectors of Nigeria and the Diaspora.

Categories of Respondents

There were 160 respondents in total: 27 persons representing 17% of the respondents were ICT top decision-makers in the Public Sector, 14 persons representing 15% of respondents were ICT top decision-makers in the Private Sector, 41 persons representing 26% of respondents were ICT personnel in the Public Sector, 22 persons representing 14% of the respondents were ICT personnel in the Private Sector, 30 persons representing 19% of the respondents are members of academia and 18 persons representing 11% of the respondents were ordinary citizens described here as End Users. See Table 4:1 and Figure 4-1.

Table 4:8 Categories of Respondents in the Study

Which of the following categories best describes your status amongst e-government stakeholders in Nigeria?		
Answer Options	**Response Per cent**	**Response Count**
ICT top decision-maker in the Public Sector	17%	27
ICT top decision-maker in the Private sector	15%	24
ICT personnel in the Public Sector	26%	41
ICT personnel in the Private Sector	14%	22
Member of Academia	19%	30
End User	11%	18
Other (please specify)		0
answered question		**160**

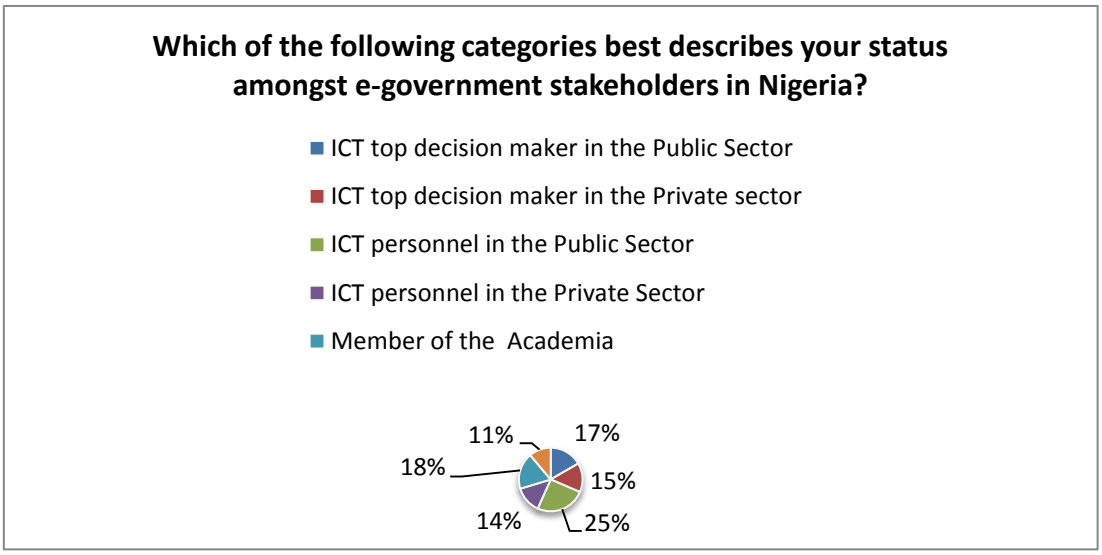


Figure 4:6 Categories of Respondents in the Study

Preference for E-Transactions against the Traditional Manual Transaction in Government

Respondents indicated that e-transactions are much more preferable compared to the traditional manual transactions in government institutions. They also provided reasons for their preference for e-transactions, describing it as more convenient, more transparent, more time efficient and that it saves cost and increases productivity, see Table 4.2 and Figure 4-2.

Table 4:9 Preferences of e-transactions over manual transactions

Do you prefer e-transactions to the traditional manual transactions in Government institutions?		
Answer Options	**Response Per cent**	**Response Count**
YES	95%	144
NO	2%	3
I can't really say	3%	5
answered question		**152**

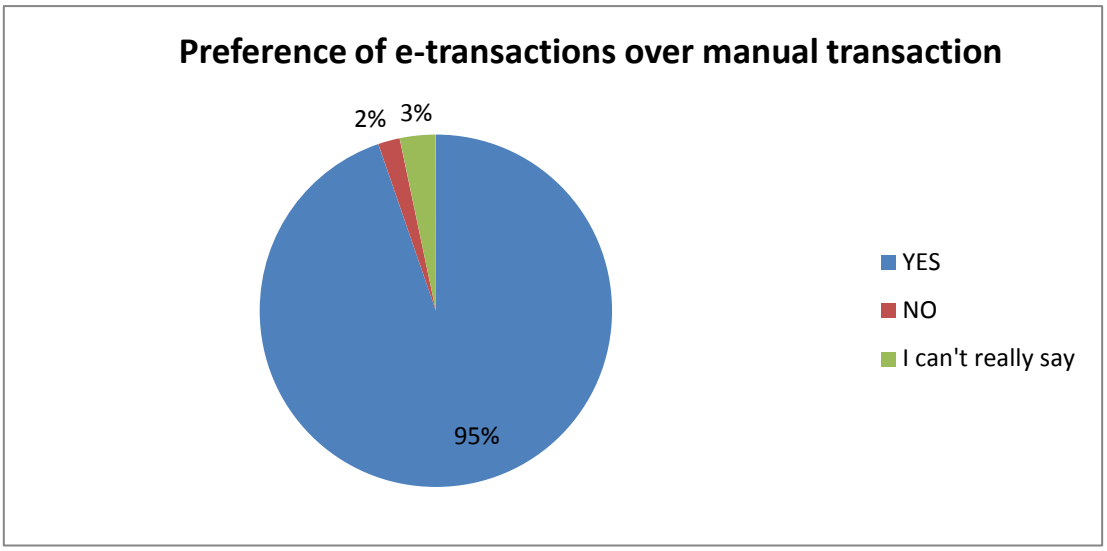


Figure 4:7 Preference of e-transactions over manual transactions

Reasons for Choosing E-Government over Traditional Manual Systems

Respondent's preference for e-government over manual traditional system of transacting government business is presented in Table 4.3 and Figure 4-3.

Table 4:10 Respondents' reasons for choosing e-government transactions over manual transactions

If your answer was Yes to Q.2 above, Please give reason(s) from the options below, otherwise move to Q.4.		
Answer Options	**Response Per cent**	**Response Count**
More convenient	53%	78
More transparent	41%	60
It saves time	35%	51
It improves productivity and saves cost	32%	47
Other (please specify)		0
answered question		**147**

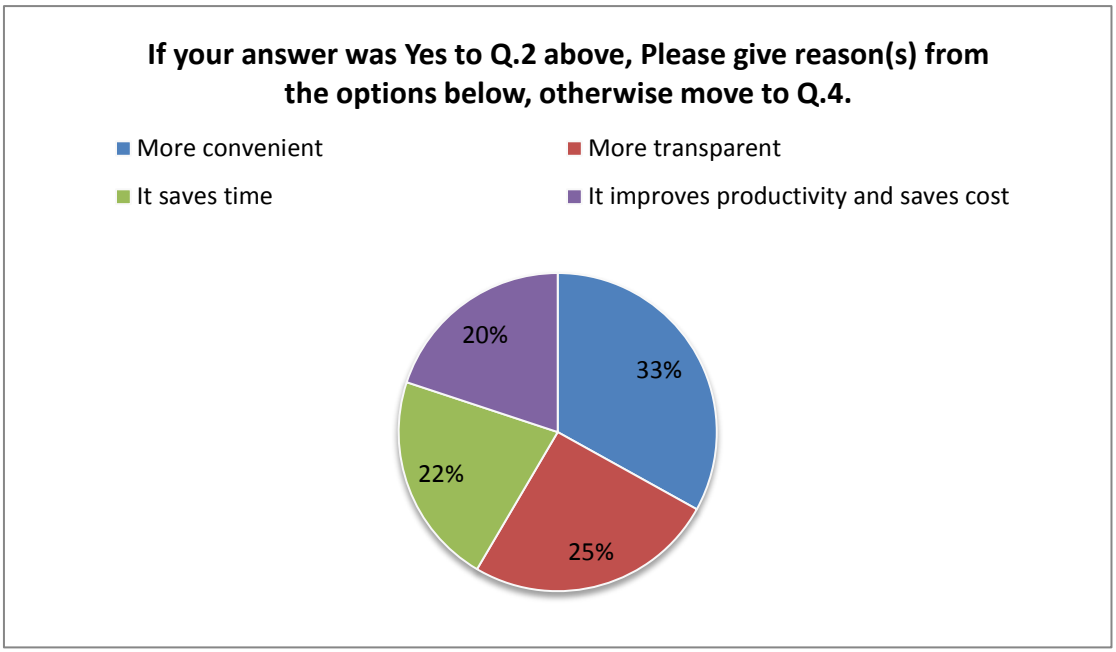


Figure 4:8 Respondents' reasons for choosing e-government transactions over manual transactions

Respondents' Satisfaction with the Present Level of E-Government Development in Nigeria

Respondents also indicated their levels of satisfaction with e-government development in Nigeria. Thirty-six persons representing 27.3% of respondents indicated that were satisfied with present level of e-government development in the country. Eighty-seven persons representing 65.9% of respondents indicated that were not satisfied the current level of e-government development in Nigeria while 9 persons representing 6.8% of respondents expressed indifference. Details are shown in Table 4.4 and Figure 4-4.

Table 4:11 Respondents' level of satisfaction with the current level of e-government development in Nigeria

Are you satisfied with the current level of e-government development in Nigeria?		
Answer Options	**Response Per cent**	**Response Count**
Satisfied	27%	36
Not Satisfied	66%	87
I can't say	7%	9
answered question		**132**

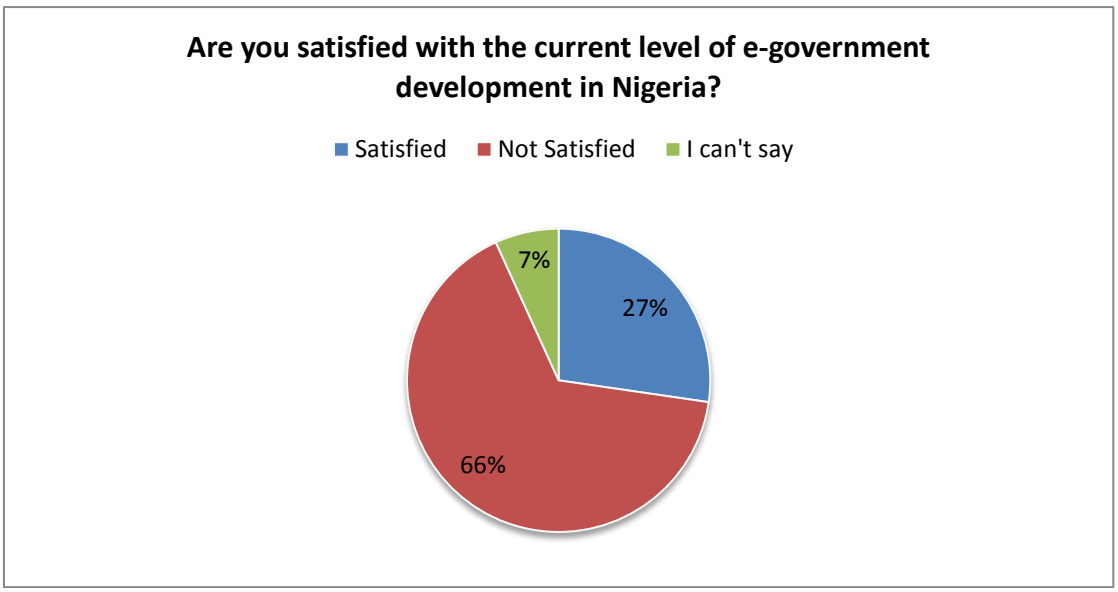


Figure 4:9 Respondents' level of satisfaction with the current level of e-government development in Nigeria

Factors Responsible For the Slow Pace of E-Government Adoption in Nigeria

A major component of the research was to find out factor(s) that could possibly be responsible for the slow pace of e-government adoption in Nigeria. The factors were listed as follows: low computer literacy level, low Internet access, lack of confidence in government initiatives, concerns over online theft and related crimes and concerns over non-prosecution of cyber-related crimes under the present laws, in case of any breach. Fifty-seven persons representing 35.4% of the respondents said the reason for the slow level of e-government adoption in

Nigeria was the low level of computer literacy in the country, 47 persons representing 29.2% of the respondents said low Internet access was responsible, 42 persons representing 26.1% of the respondents said citizens lack confidence in government initiatives, 67 persons which represents 41.6% of total respondents said concerns over online theft and related online crimes could be responsible, 44 persons representing 27.3% of the respondents said concerns over prosecution of cyber-related crimes under the present laws in case of any breach could be responsible, while 52 persons representing 32.3% indicated that all of the factors presented above could be responsible for the slow pace of adoption of e-government in Nigeria. See details as shown in the Table 4.5 and Figure 4-5.

Table 4:12 Factors responsible for the slow pace of e-government adoption in Nigeria

What do you think may be responsible for the slow adoption of e-government by citizens of Nigeria? You can choose more than one option.		
Answer Options	**Response Per cent**	**Response Count**
Low computer literacy level	35%	57
Low internet access	29%	47
Lack of confidence in Government initiatives	26%	42
Concerns over online theft and related crimes	42%	67
Concerns over prosecution of cyber related crimes under the present laws, in case of any breach	27%	44
All of the above	32%	52
None of the above	1%	2
Other (please specify)		0
answered question		**161**

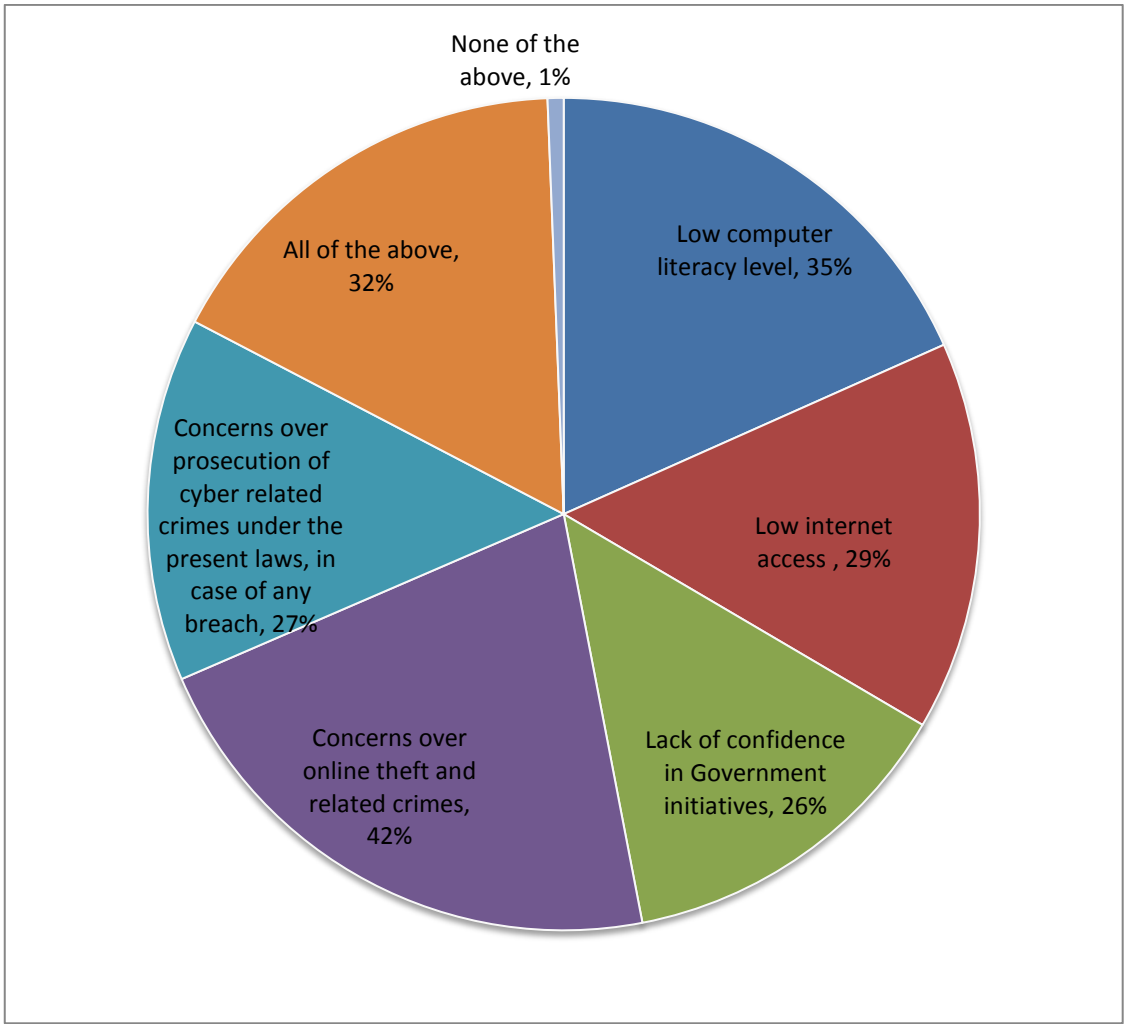


Figure 4:10 Factors responsible for slow pace of e-government adoption in Nigeria

Security and Privacy Concerns in the Consideration of E-Government Adoption in Nigeria

The researcher thought to find out if security and privacy concerns are considered paramount while considering e-government adoption in Nigeria. Fifty-five persons representing 33.5% of the respondents said security and privacy concerns are most paramount, 45 persons representing 29% indicated that security and privacy concerns are more paramount, 47 persons representing 30% said they are paramount, while 5 persons representing 3.2% said security and privacy concerns are not paramount, and 3 persons representing 1.9 indicated 'none of the above' expressed indifference. Details are shown in Table 4.6 and Figure 4-6.

Table 4:13 Respondents' concerns over security and privacy in the consideration of e-government in Nigeria

Can you say that security and privacy concerns are paramount while considering e-government adoption in Nigeria?		
Answer Options	**Response Per cent**	**Response Count**
Most Paramount	36%	55
More Paramount	29%	45
Paramount	30%	47
Not paramount	3%	5
I can't say	2%	3
	answered question	**155**

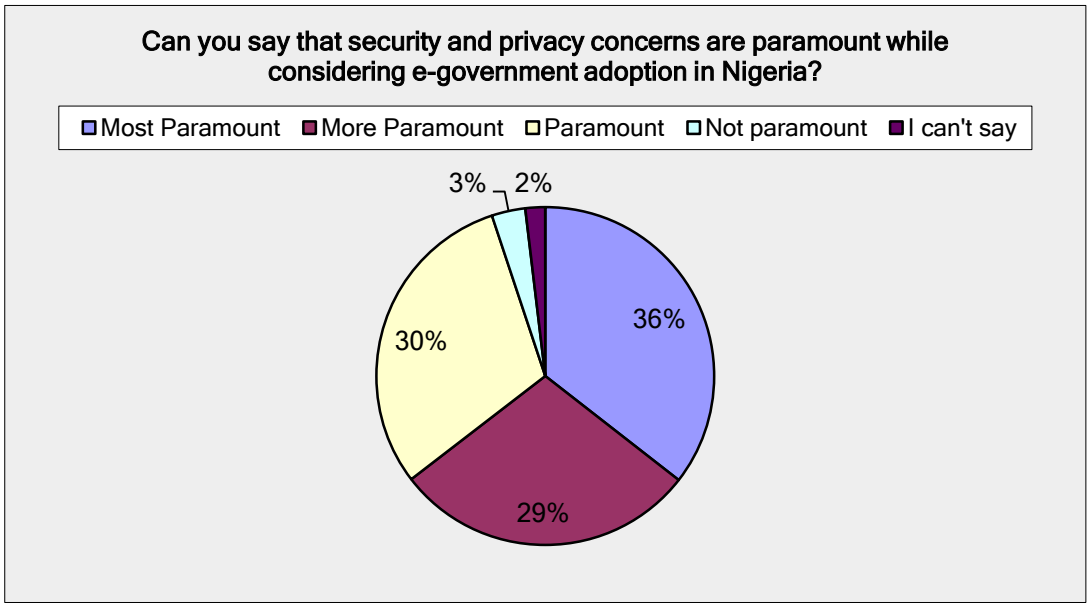


Figure 4:11 Citizens' concerns over security and privacy in the consideration of e-government in Nigeria

Integration of a Security Framework into E-Government Implementation Strategy

Opinions of respondents were sought regarding the integration of security framework into the nation's e-government implementation strategy from the outset, not as an add-on. One hundred and twenty-three respondents representing 80.9% strongly recommended the integration of a security framework, 14 respondents representing 9.2% did not recommend the integration

of a security framework and 15 respondents representing 9.9% simply indicated 'I can't say' See details in Table 4.7 and Figure 4-7.

Table 4:14 Level of support for the integration security framework in e-government implementation strategy from the outset

In the nation's e-government implementation strategy, will you recommend that an e-government security framework be integrated from the outset and not as an add-on?		
Answer Options	**Response Per cent**	**Response Count**
I strongly recommend	81%	123
I don't not recommend	9%	14
Indifferent	10%	15
answered question		**152**

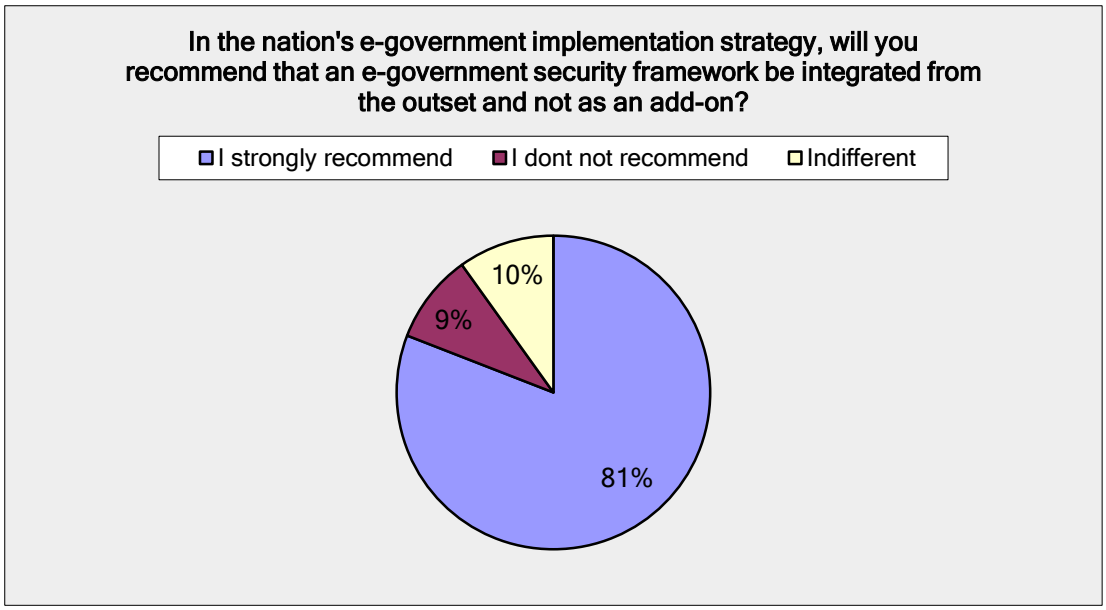


Figure 4:12 Level of Support for the Integration Security Framework in e-government Implementation Strategy from the Outset

Findings

It was evident from the survey that respondents prefer e-transactions much more compared to the traditional manual transactions of government. Stating that it is more convenient, transparent, saves time and cost. More interestingly, about 27% of the respondents said they were satisfied with the level of e-government development in Nigeria while 65% of the respondents were not satisfied. The study may not have been very useful if the researcher had not sought to find out why a greater percentage of the respondents expressed dissatisfaction in the current level of e-government development in the country. It was indicated that concerns over online theft and related crimes were considered a predicament in the development or adoption of e-government in country with about 41% of respondents attesting to that. Similarly, 94% of respondents indicated that security and privacy concerns are paramount in the consideration of e-government implementation.

From the above analysis, it is apparent that security and privacy related concerns are a major concern about the adoption of e-government in Nigeria. The questionnaire offered questions relating to security and privacy in several ways so as to measure consistencies in their responses. It was confirmed that respondents were sure of what they indicated at every given instance. Therefore, the pragmatic approach adopted in this research is the most appropriate, given the fact that it affords me the freedom to use any method that is relevant to achieving the desired objectives.

In this situation as evident in the data illustrated above, a security framework has to be designed as a component of the e-government adoption strategy, adapting relevant international industry standards so as to serve as a reference to government organisations during the implementation of e-government in Nigeria.

In addition to the above, literature updates were carried out according to the reference areas, e.g. e-government strategies, IT security legislations and policies. After the framework was designed, a framework validation was carried out. The

validation approach was to seek expert opinion; experts in the industry given an opportunity to evaluate the framework and give comments according to prescribed questions to enable easy analysis and reporting. Experts were selected from top decision-makers in ICT departments in the public sectors, top decision-makers in ICT departments in the private sectors, ICT personnel in the public sectors, ICT personnel in the private sectors, and members of academia some of whom participated in the initial survey. The analysis did not focus on the status of respondents as it was considered not to have influenced their responses, since the questions were generic in nature and not specific to groups within the population. Every participant irrespective of status was considered a user of e-government services as well as a citizen of Nigeria.

Discussion of Research Process Flow

The research process flow shown in Figure 4:11 illustrate basic steps or procedures that were followed to accomplish the research outcomes in this thesis. The first process was the formulation of the research problem: to single out a particular research area from general knowledge to a specific subject matter. It requires thorough understanding of the problems and articulation of questions for investigation, it is a critical process, the foundation on which everything else was built. The next step was to carry out a review of all available literature so as to be well-acquainted with existing theories as well as published empirical reports on the subject or related topics.

The outcome of the literature review gave the researcher the knowledge as to the materials and data available to enable him to spell out the research contextually. During the review, the researcher diligently ensured that background facts came from authorized sources so as to avoid reporting invalid outcomes. Academic conference proceedings, academic journals, books, reports by governmental agencies and authorities, published media articles and other library resources were useful sources in this process. After the literature review, several initial facts were established leading to what was described as the conceptual framework.

The conceptual framework arose from well-established facts or data from secondary sources upon which certain decisions have been made, it defined key factors that brought about the supposition of this research; it gives an interpretative approach to the concept of the research. The information in the conceptual framework guided the research design and the nature of data to be collected. The researcher collected and analysed both qualitative and quantitative data systematically; the goal was to ensure better evaluation so that the short-comings of one type of data are made up by the advantages of the other. Though in this research the data was gathered sequentially, after carrying out the qualitative part through interviewing, the outcome of the analyses was used to develop a questionnaire for quantitative data analysis. The outcome of the investigations pointed to a research problem to which the researcher recommended a solution.

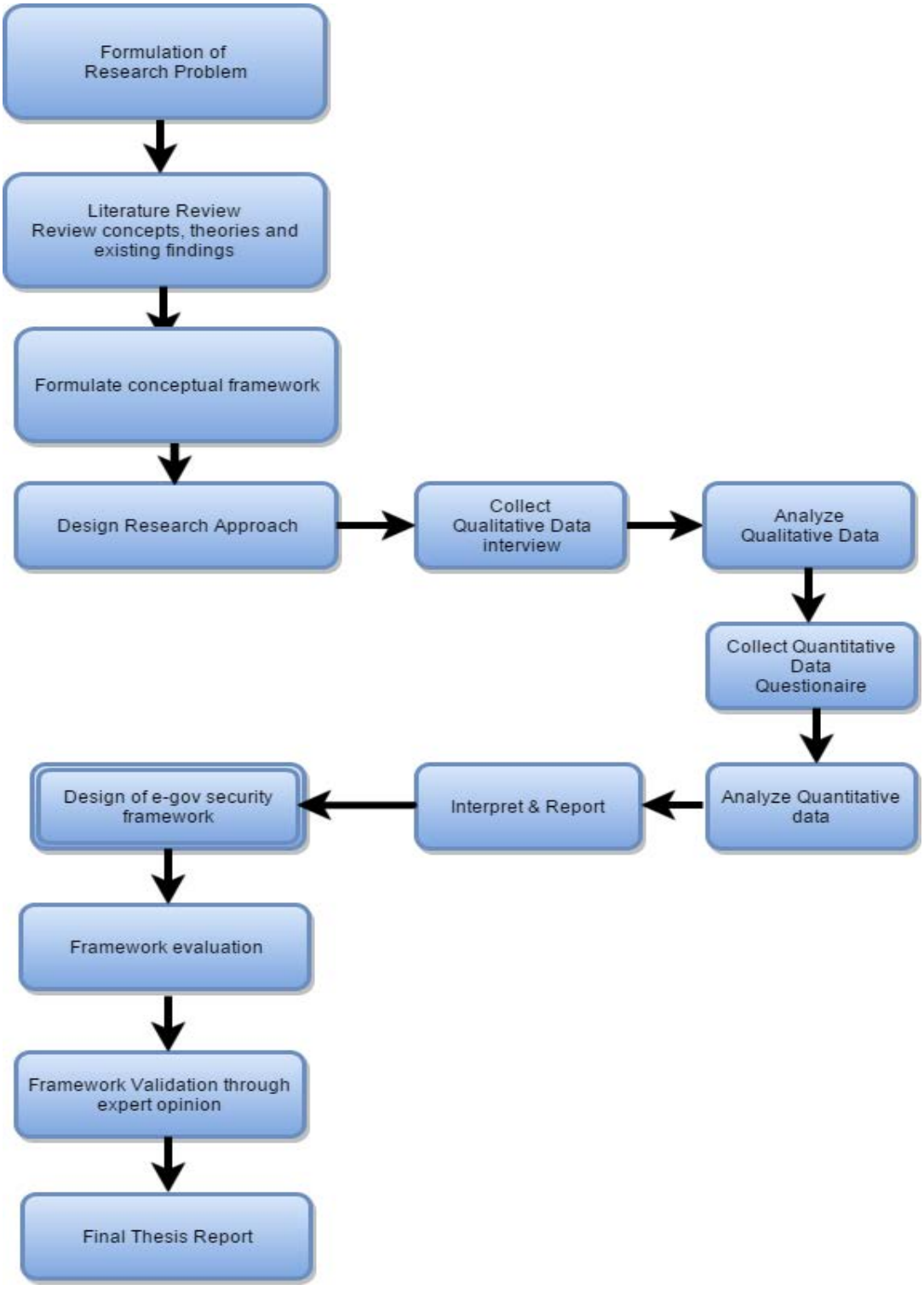


Figure 4:13 Research process flow

The findings from the research indicated that security and privacy concerns were responsible for the slow pace of e-government adoption in Nigeria therefore the researcher developed a strategic framework for e-government security in Nigeria. After the design, the framework was taken back to those professionals (experts) that participated in the initial survey for their expert opinions; a process known as evaluation and validation of the framework. Their opinions were also analysed and their observations and suggestions were reported accordingly (see appendix III). After these whole processes of Problem formulation, Literature review, Data collection and analysis, Framework design, Framework evaluation and validation, it came to the final stage of writing the thesis report.

Security Regulations, Standards, Frameworks and Compliance Issues

Introduction

To solve the problem of information security as identified by the study conducted and reported in the previous chapter, this chapter introduces the relevant information security regulations, standards, frameworks to be considered in the proposed framework for e-government security. Information security undertakes a vital role in protecting the data and assets of organisations, particularly as it has to do with security incidences, such as the defacement of websites, server hacking and data leakages. Therefore, there is a need for government organisations to be fully aware of the importance of dedicating additional resources to the protection of information assets.

In dealing with the situation, a number of governmental and non-governmental organisations have set up benchmarks, standards, legal and regulatory frameworks and strategies on information security to make sure an appropriate standard of security is sustained, resources are utilised tenaciously, and ensuring that the best security actions are implemented.

In this chapter, some of the most commonly adopted standards and regulations for information security are discussed, as relevant to this research. E-government security frameworks by other researchers are also evaluated and an adaptive e-government security framework to NIST cyber security introduced. This chapter also seeks to look into existing frameworks demonstrated by other researchers in different countries, with an effort to locate its strengths and palpable weaknesses in several unique areas of deployment.

Policy

According to the SANS Institute (2014), policies are characteristic documents that outline definite rules that should be adhered to. In IT, policies are defined to specific purpose, therefore different policies covers different unique tasks. For instance, the

"Acceptable Use" policy covers the rules defining the proper use of the information technology facilities.

Standard

A standard is characteristically a set of system-specific or procedural-specific requirements that should be followed by every personnel in the field (SANS, 2014).

Guidelines

Guidelines are usually a set of definite procedures put in place to achieve specific goals or objectives; it could be technical or non-technical. They may not be compulsory but highly advisable. Valuable security policies always refer to standards and guidelines that have been provided to serve as a guide to achieve desired goals (SANS, 2014).

Information Security Policy

Information security policies are usually sophisticated, non-technology specific, risk control instructions or procedures and list of consequential actions or countermeasures where certain policies are not followed. However, this is not the same with the information that is unique to the implementation that requires guidelines, standards and procedures. Top decision-makers in the managerial or executive levels of an organisation drawn from various departments come together to outline relevant guidelines and standard practices (Rees et al., 2003). It is therefore important for every establishment to have a comprehensive information security policy.

Information Security Standards (International and National)

Information security standards are also referred to as voluntary standards, or possibly frameworks: a collection of processes that have been listed and circulated by renowned global organisations, and are generally accepted by practitioners in the field of information security profession as a guide.

Generally renowned ones are as follows:

I. Control Objectives for Information and related Technology (COBIT)
II. International Organization for Standardization (ISO) 27001 and 27002
III. (US) National Institute of Standards and Technology (NIST) standards.

COBIT

COBIT is published by ISACA, the Information Systems Audit and Control Association. ISACA is a renowned independent IT governance organisation, its guidelines are used by IT managements in many organisations to define and manage processes based on a maturity model like the COBIT 5 Capability Maturity Model (CMM). COBIT is not particularly about information security, it is an all-embracing IT standard, but certain security practices are embedded within it.

COBIT has a higher-level set of information security guidelines than the ISO 27000 series, which proposes to align business goals with IT goals. ISACA periodically updates the COBIT processes and releases new versions. COBIT 4.1 is structured around four conceptual areas, referred to as domains, analogous to the preferred order an organisation would use to implement security program components along the lines of the well-known Plan, Do, Check, Adjust (PDCA) growth cycle commonly used to build and continuously improve services.

ISO 27000 Series

The ISO 27000 series of information security standards presents a set of frameworks for developing a security programme from initial conception to maturity. It is subdivided into parts to enhance manageability, each part laying down a set of activities that belong to phases comparable to those in the Plan-Do-Check-Act (or more accurately, Plan-Do-Check-Adjust) (PDCA) cycle, as in COBIT (Rhodes-Ousley, 2013).

ISO 27001 is a high-level specification for the management of an information security programme. This is known as an information security management system (ISMS). ISO 27001 standard contains high-level statements about management

responsibilities such as defining objectives, measuring performance, and auditing compliance. It includes provisions to instigate a risk to determine which controls are the most important for each organisation, and how fully they should be applied. In principle, this is to some extent similar to COBIT's Plan and Organize concepts or the Plan concept of the PDCA cycle.

ISO 27002 is a complete set of information security controls that would perfectly be driven by the output of the risk assessment performed as part of ISO 27001. This standard forms a complete reference to all the things an organisation might want to do. It can be viewed as a set of best practices, and it is up to each organisation to determine which of them apply to their business environment. This can be viewed as somewhat similar to COBIT's Acquire and Implement concepts or the concept or the "Do" part of the PDCA cycle.

ISO 27003 is designed to provide recommendations and best practices to implement the ISMS management controls defined by ISO 27001, in other words, how to deliver the security programme. This can be compared to the Deliver and Support concepts of COBIT, or the Check part of the PDCA cycle.

ISO 27005 classifies a risk management framework for information security that can be used to inform the decisions within ISO 27001 that lead to selection of controls for ISO 27002.

NIST

The US National Institute of Standards and Technology (NIST) provide a collection of "Special Publications" to help industries, governments, and academia with standard practices. One of such publications is the "800 series" this set of security-specific publications is very specific to individual technologies, with the exception of 800-53. 800-53 was developed primarily for the US Federal Government, to be specific about security controls and structures, security measures, common paradigms, risk management, information system categorization, security control selection, and monitoring of security controls. 800-53 is organised into 18 "security control

families," which are conceptual categories that represent important components of a complete security program (NIST, 2014b).

NITDA

The National Information Technology Development Agency (NITDA) of Nigeria is an agency of government which derives its mandate from the NITDA Act of 2007 for the development of information technology throughout Nigeria, by formulating operating and regulatory framework/policies, guidelines, standards, and other incentives for the advancement of IT in the country. The act also mandates NITDA to make sure there is security in Nigerian cyberspace including the secure and efficient implementation of an electronic government programme (National Information Technology Development Agency, 2013).

Several government organisations have already moved their fundamental services online. Presently, information technology is driving service delivery in the country, making the information technology infrastructure critical.

NITDA offers the government a general standard and guidelines on national information technology systems and network security. These standards are compulsory for all federal, state and local government agencies and institutions as well as private sector organisations which own, use or deploy critical information infrastructure of the Federal Republic of Nigeria. They serve as reference for systems auditors, network administrators and security personnel, among others. Additional security guidelines may be developed and used at the agency's discretion in accordance with these standards (National Information Technology Development Agency, 2013). The guideline is known as the National Information Systems and Network Security Standards and Guideline, and they are mandatory for all the tiers of government, the local, state and federal; all the arms of government, its agencies and institutions, the private sector and every entity that operates critical information infrastructure within the Federal Republic of Nigeria. Ministries, Agencies and Departments (MDAs) of government are expected on a quarterly basis to report their compliance to the relevant directorate in NITDA. It sets out minimum standards for Information Categorization, Intrusion Detection and Prevention

Systems, Minimum Security Requirements, Protection of Sensitive Personal Information (Object Identifiable Information), Security of Public Web Server, Firewall Systems as well as Cyber Forensics. Apart from the basic principles of information security, which are confidentiality, integrity and availability, survivability and continuity business processes were added as a vital component (National Information Technology Development Agency, 2013). Its data security measures include: data protection and access control, encryption, backup and recovery processes/procedures, change and control processes, data disposal and retention requirements, storage and audit controls.

1.4 Security Threats and Vulnerabilities Management

Security Threats

As earlier described in section 2.16, security threats are considered to be incidents that may be either intentional or unintentional that have the propensity to cause harm or have adverse effect on critical information technology infrastructure (ISO/IEC, 2014). Any activity that tends to exploit definite vulnerabilities within e-government systems is a threat to the system (Karokola et al., 2013). According to Karokola et al. (2013), threats may possibly stem from artificial or natural disasters. Artificial threats may involve incidents that may occur due to human errors or deliberate forms of attack; all forms of attacks whether deliberate or not have the potential to adversely affect e-government services. Security threats are managed in compliance with security regulations, framework and standards.

Security Vulnerability

Security vulnerabilities are errors or weak links within an information system infrastructure; they could either be in the hardware or in the software. It is a system characteristic that provides the opportunity for threats to happen; it can also be described as a system's exhibition of undesirable characteristics (Newman, 2006). Any aspect of the system can open a weak link from where an attacker can gain access to internal processes and controls. There are several ways through which an attacker can exploit the vulnerabilities of a system as there are various system

vulnerabilities. Vulnerability could either be as a result of an error in configuration or what is referred to as default configuration weakness. Although new vulnerabilities are always discovered in system applications and patches are also published by authors of those applications, it is difficult for government organisations or professionals to keep pace with security publications regularly. Therefore attackers seem to take advantage of the time lag between the vulnerability and the installation of a patch to exploit systems (Hossein Bidgoli, 2006).

ISO/IEC 27000 Family: Code of Practice for Information Security Management

The ISO/IEC 27000 family is about the most commonly referenced code of practice for information security and management. It relies upon ISO 17799. The ISO 27000 series gives standards for best practice procedures about system design, information security management as well as information security controls (ISO/IEC, 2016). It includes: ISO 27001 which comprises information security management systems requirements certification standard/specification plus standards for establishment, implementation, control and advancement of the information security management system (ISMS). ISO 27002 presents the code of practice for the management of information security with a complete set of controls for information security. Its goals and a set of universally recognised practice (ISO/IEC 17799) were reviewed last in 2005 and were given a new name as ISO/IEC 27002:2005. ISO 27005 was intended to offer security guidance on information risk management (ISO/IEC, 2016). The twelve guiding security control principles of the ISO/IEC 27002 are as follows:

- Risk evaluation and management: it lays down guidelines in carrying out risk evaluation and management. It involves a methodical method for the assessment of threats as well as vulnerabilities, while contrasting evaluated risks with recognized risk criterion
- Policy on security: provides direction to the security management

- Information security organisation: gives a detail description of how every in-house security components could be structured
- Management of assets: present best methods for classifying resources
- Securing human resource: gives direction to security related issues with respect to personnel both newly employed and those retiring
- Securing physical assets: guides on the physical security of system hardware
- Communications and operations: offers guide on the management of technical security controls in systems and networks
- Control of access: gives a guideline to restrict rights of access to system resources
- Information system acquisition, development and maintenance
- Information security incident management: gives proper guide on the way to act in response to security breaches
- Handle business continuity: provides a guide for the protection, maintenance and restoration of business-critical processes and systems
- Compliance: ensures conformity with information security policies, standards, guidelines, laws and regulations (ISO/IEC, 2016).

Legal Considerations

When a country wants to adopt e-government, one of the major challenges they face is the identification of relevant laws, where there are no laws, new legislations have to be put in place, because for e-government processes to be successful, its processes has to operate under a legal framework. Apart from the legal framework of the respective countries, it must not also violate international laws. For instance the utilization of a digital signature in a country must be enforceable under the relevant international laws (International Telecommunication Union, 2009).

There must be a body of laws regulating the authentication of participants in the process so as to guarantee citizens' privacy protection (International Telecommunication Union, 2009). There are other situations where laws have to be amended to allow for electronic evidences in court, because until very recently

electronic evidences were not admissible in the courts in most countries even when electronic financial transactions were been legitimately carried out.

Security Considerations

Government and businesses all over the world have persistently been plagued by cyber related threats, due to increased attention to online assets. Criminal minds have improved on their technical skills to perpetrate these unwholesome practices. The challenge has taken a global dimension and therefore requires a globally accepted approach to putting these criminals in check. ISO/IEC 27001 offers a common management framework for the assessment and management of risks that may emanate from Internet flaws or human involvements (Humphreys, 2013).

Sensitive governmental and citizens data are processed, transmitted and stored using computer systems or devices. Citizens rely so much on these computer devices to provide them with on-demand services but these devices are faced with a variety of threats. These threats keep on increasing as there are obvious over-dependence on digital storage, processing and transmission of information.

Attackers are becoming more ambitious, they are driven by financial gains rather than mere notoriety as was previously perceived. To tackle the menace is to more than a question of just employing a plug and play security tool; it requires a deliberate, all-encompassing security strategy peculiar to a given situation at a given time.

Framework Definition

Generally, a framework is described as a genuine or theoretical composition planned to be a supporting guide or structure in the development of anything that could be improved or expanded to a more useful structure in the future (Rouse, 2015). From the information technology perspective, frameworks are principally structures with multiples layers that specify the types of applications that are suitable for a given purpose and how they can integrate.

A framework can contain series of functions in the system and directs the processes of integration; integrating the operating system layer with the application subsystem layer as well as the standardisation of the network communication layer. Frameworks are usually more prescriptive and inclusive than structures (Rouse, 2015).

Significance of a Framework in the Implementation of E-Government Security

One cannot overstate the immeasurable advantages of employing a framework in the plan to control cyber threats: it is not enough to deploy technical solutions, but a prudent management of strategies that are most instructive to know who handles what at a given time, the inculcation of personnel's skills improvement training are also very important (Humphreys, 2013).

A security framework should be capable of accomplishing the following:

- Operate within the country's data protection/privacy laws and international standard practice
- Protect the interest and privacy of users and stakeholders
- Define rights and privileges of users (access control)
- Identify possible sources of threat (risk assessment)
- Indicate security awareness training
- Have sufficient plans to defend the system against potential threats (mitigation plans)
- Be able to quickly discover the source of an attack when it occurs
- Have the ability to swiftly act in response to an attack, and should know what to do in face of an attack
- Recover from the effects of the attack and get the system restored to normalcy and ensure the continuous availability of e-services
- Routinely evaluate processes and compliance issues.

Existing E-Government Security Framework Developments

Some researchers have presented papers on the subject of e-government security frameworks mutually considering the developed and developing countries, some of them are highlighted here. Gamlo et al. (2009) reported that the UK e-government security strategy framework showcased a policy guideline; it was an outstanding broad-spectrum framework for security provision for e-government projects. They argued that the framework outlined security goals, potential security risks as well as e-government security services developments that demonstrate concerns for the processes of registering users, because the system was designed so that any new user must register his credentials, the credentials will be used for subsequent authentication as there will now be a user profile for that particular user. The validation or authentication will be based on his registered profile (Gamlo & Bamasak, 2009). They stated that the framework also took into consideration the common possibility of people using false identities during registration therefore making the system to allow a wrong person have access. They made provision for a countermeasure in the framework as well. The framework also considered services that may be affected by issues of trust when carrying out e-government transactions (Gamlo et al., 2009). The researcher also suggested the application of a public key encryption in the course of implementing a conventional PKI and digital certificates.

In a related report, Choi and Chun (2013) discussed a framework development involving the Public Administration Information Sharing Centre, South Korea called SecureGov. It was a security framework for the implementation of a secure way to share citizen's data for the delivery of governmental services, particularly in Government to Government communications (Choi and Chun, 2013).

The SecureGov security framework by Choi et al. (2013) claimed to be a universal solution that can solve e-government security issues in every country. Choi et al. (2013) made a particular reference to a situation where the government of United State of America abandoned a project to build a centralized system for data sharing and also includes a central government database which has been on-going for

three-years. It was planned to enable government manage the process of information sharing among departments particularly records of citizens or residents (Choi and Chun, 2013). Chin and Chun concluded that the failure was attributable to several issues, issues relating to the complex nature of connecting different systems located in dispersed areas. There was later a change of strategy; the new plan designed a system where every government department saves its data on a central server known as a data warehouse.

SecureGov approached the problem utilizing the distributed service oriented architecture, a situation where every data is stored at its location, and will be transmitted on request, the SecureGov framework has some advantages with user control and easy access to relevant citizens data but the notable disadvantage of the security framework was a situation involving unauthorised personnel prying on citizens sensitive personal information; this was a major problem that was not effectively dealt with by the framework.

Karokola et al. (2013) presented a framework in his research titled “Framework for securing e-government services – a case of Tanzania”. First they identified that e-government maturity models (eGMMs) were very important in the design of a framework for the Tanzanian national e-government strategy. eGMM was used as an instrument for setting a benchmark and guideline for e-government implementation and delivering of government services. Though, the maturity models seem to be deficient of technological and non-technological security services at every stage of maturity, which has led to a disorderly strategy between e-government day to day services and security services. To solve the problem arising from the wide security services gap that exist in eGMMs, there was a proposal for the design of a framework for securing e-government services that will integrate IT security services into maturity stages of eGMMs. Setiadi et al. (2013) also proposed a framework that they claimed to be very comprehensive; the framework was referred to as a balanced e-government security framework (BEGSF). It consists of several layers namely:

- Asset layer,
- Requirement layer
- Protection layer

The objectives of the framework as illustrated in diagram in the requirement layer contains the basic criteria of security known as the CIA triad; see Figure 5-1. The purpose of the framework was to make sure that every e-government service and processes are protected with the same amount of security. It is a combination of technological and non-technological approach in securing e-government transactions (Setiadi et al., 2013).

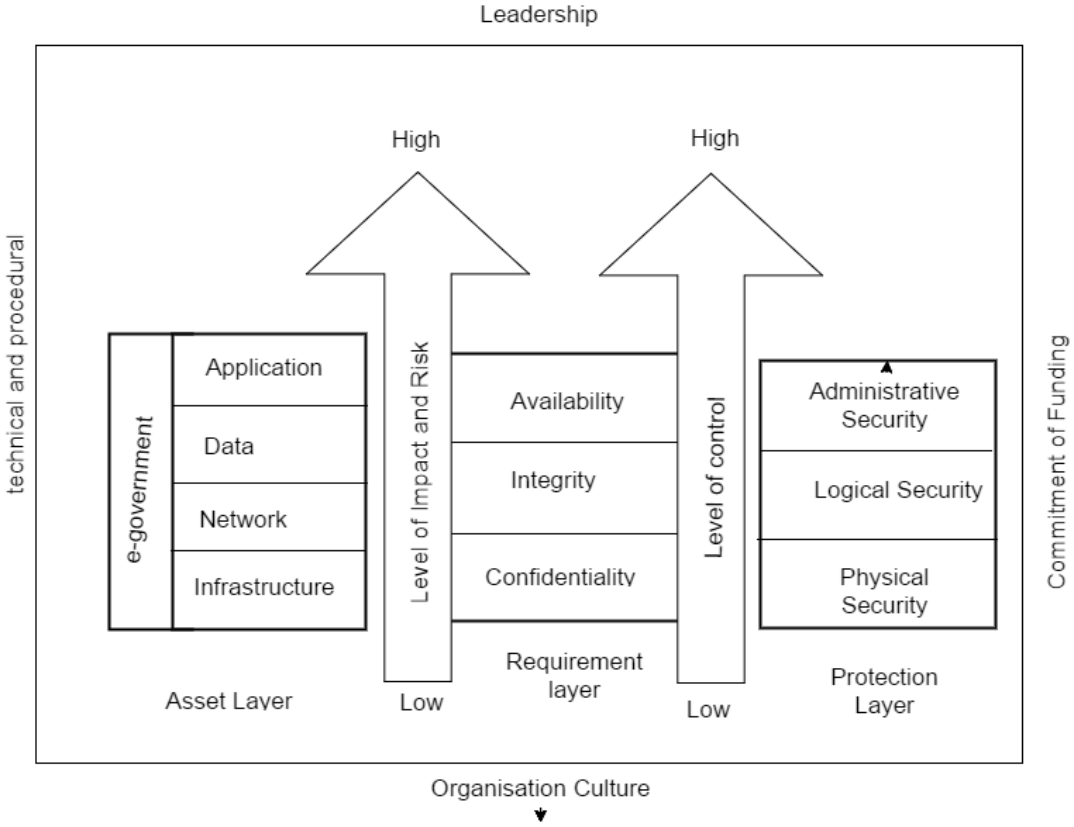


Figure 5:14 Balanced E-government Security Framework Diagram (Setiadi et al. 2013)

Al-ahmad et al. (2008) authored a framework known as the extended security framework for e-government. The framework has its main point in the advantage that it tends to include every part of e-government security: the people, the process and the technology.

The people aspect involves the individuals using the e-government, the training and sensitization of the public concerning the issues related in e-government. The administration and management of policies governing security procedures is referred to as the Process while the components that put into effect the security implementation is the technology (Al-Ahmad et al., 2008). The structure is illustrated in Figure 5-2.

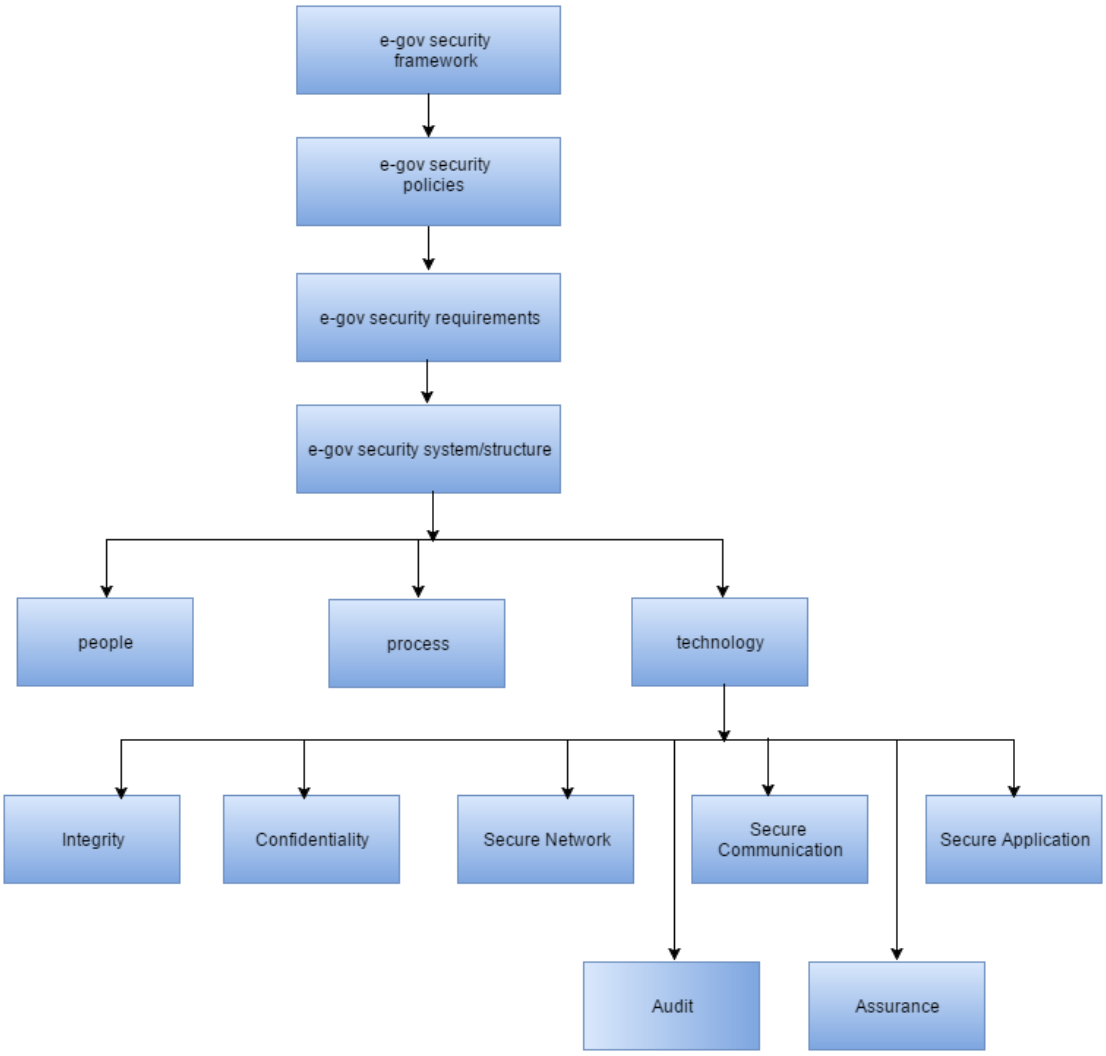


Figure 5:15 Extended Security Framework for e-government by (Al-ahmad et al. 2008b)

Gamlo et al. (2009) also proposed a guide to the security of e-transactions within e-government systems in the kingdom of Saudi Arabia utilizing the concepts of PKI, having an in-built security system that guarantees different layers of security measures and are built to be interoperable. The fundamental transactions of

services are carried out effectively in a secured manner utilizing cryptographic techniques.

Observations

All the frameworks evaluated provided for secure authentication and secure transactions but there were no provision for or consideration of the survivability of the e-government system in case of an attack. E-government services when deployed are expected to be available 24/7; therefore a viable e-government security framework must be designed to make room for government services continuity in the situation of any systems failure or possible attacks.

Recommendation for the Adoption of the National Institute of Standards and Technology (NIST) Cyber Security Framework (2014) into the Strategic Framework for E-Government Security in Nigeria.

In proposing full scale adoption of e-government in Nigeria, it is expected that all critical infrastructures are reliable and dependable otherwise the nation's e-government implementation will be at risk. Therefore it was recommended that the cyber-security risk management standards of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-395, International Organization for Standardization (ISO) 31000:20093 and ISO/IEC 27005:20114 frameworks should be adapted into the Nigeria's e-government security strategic framework so as to provide a more flexible and risk-based implementation of e-government in Nigeria.

The Framework is an advanced approach to mitigating or managing security threats associated to e-government; it comprises three significant parts as demonstrated in following:

1. The Framework Nucleus
2. The Framework Implementation Levels
3. The Framework Outline

Every framework component strengthens the connection between e-government services drivers and e-government security strategies as described in below:

The Framework Nucleus is a collection of information security actions, expected results and relevant references that are universal amongst critical e-government infrastructure components. The nucleus provides industry standards, guidelines and practices in a way that permits communication of security actions within the government departments starting from the executive level to the implementation, and operations levels. The Framework Nucleus comprises five simultaneous and continual functions namely: Identification of threats, Protection or defence of the system against threats, Detect risks factors, Respond or counter the risk, Restore the system to normal operations (NIST, 2014a, p.4).

In a joint or contiguous study, these functions offer an advanced, strategic analysis of the life cycle of a government's handling of security threats.

The Framework Nucleus subsequently analyses basic main categories and subcategories for each function, therefore linking them with some useful references like contemporary guidelines, standards, principles and practice for every subcategory.

The Framework Implementation Levels give perspective on how the government views impending threats to security and the processes in place to handle such threat. Levels here refer to the scale to which government should handle security risk and management activities and express the characteristics defined in the security framework (NIST, 2014a, p.5). The levels characterize practices over an array, from Partial (level 1) to Adaptive (level 4) (NIST, 2014a, p.5). Levels such as these demonstrate a succession from casual, spontaneous responses to reactions that are active with quick response to security risk. At the time of level selection, current security risk management practices of the government organisation should be considered, the threat situation, legal and regulatory requirements, policy direction, services/business objectives as well as constraints (NIST, 2014a, p.5).

A Framework Outline characterizes the outcomes according to service requirements that a particular organisation may have chosen from the framework categories and subcategories. This framework outline can be described as the

configuration of guidelines, standards, and actions of the framework nucleus in a fastidious implementation situation (NIST, 2014a, p.5). The framework outlines may be employed to recognize chances for convalescing a security position by drawing comparison between a 'Current' report/the Present state and a Target report/the Goal state (NIST, 2014a, p.5).

To come up with a report, a review of all the categories and subcategories can also be made, according to service drivers to establish what is most important; implementers may include categories and subcategories as may be deemed necessary in addressing the security risks. This Current Outline may then be employed to ensure priority is given as well as measurement of advancement towards the Target report, whilst considering other service requirements as well as cost implications and novelty. The Framework Outline can be used to carry out internal assessment and communicate within an e-government structure (NIST, 2014a, p.5).

Management of Threats to E-Government Security

The Framework for security management is a continuous practice of analysing, measuring and responding to security incidences. In dealing with associated threats, there should be a versed understanding of the propensity of security breaches and the consequential impact of such occurrences. Consequent upon the foregoing, government agencies and departments may find out the tolerable risk level for delivering services, therefore articulating them adequately by giving them respective levels of tolerance to potential risk. Base on understanding of security risk tolerance, the government may give priority to e-government security activities, which will enable departments to make critical decisions about information security overheads according to the requisite knowledge (NIST, 2014a,p.5).

Total implementation of information security risk management programmes presents government businesses with the responsibility to measure and make adjustments to their security programmes. Government can choose to manage risk with diverse approaches, they could choose to mitigate the risk, transfer the risk,

circumvent the risk, or accept the risk; however this depends upon the possible impact on essential service outcomes (NIST, 2014a,p.5).

It provides support for persistent risk evaluation and verification of service drivers to assist government to decide on target states with respect to security activities to give expected result.

Therefore, the Framework offers government the capacity to choose dynamically and make improvements in the security risk management for e-government deployments.

Framework Fundamentals

The Framework provides a universal underlying factor for the appreciation, management and the communication of e-government security risk from both internal and external perspectives. It is considered to be a useful tool in identifying and prioritizing actions for tackling threats to e-government security; it is also considered a very useful tool for the alignment of policies, businesses, and technological methods in the management of such threat. It could be employed to handle e-government security risk in the entire government or directed to focus on the delivery of essential services between government to government (NIST, 2014a, p.7).

Framework Nucleus

The Framework Nucleus presents series of actions to accomplish a definite e-government security outcome. The Nucleus does not necessarily represent a checklist of steps to be carried out. It basically represents key e-government security outcome identified as useful in the management of threats in e-government (NIST, 2014a,p.7).

The Nucleus consists of the following fundamentals, namely:

- Functions
- Categories
- Subcategories
- Instruction References

The Framework Nucleus has several functions and they function side by side as follows:

- Identify
- Defend
- Detect
- Act in response
- Restore

The framework nucleus will help government departments in expressing their management of security risk by classifying information, ensuring that the right decisions are made in terms of daunting security risk management, addressing threats, and to ameliorate matters by making relevant adjustments based on previous experience.

The Functions also line up with existing methodologies for the responding to incidences and to demonstrate the inherent advantages in investing so much in information security.

Functions need to be subdivided into small definite and precise actions in order to achieve the required security conditions, these subdivisions of activities are referred to as Categories or function classification. Some the examples of these functions classification includes: access control, asset management and process detection (NIST, 2014a)

A further division of a category into smaller definite outcomes that involves more detailed technical and management processes is referred to as Subcategory. This subcategory help maintain the required security conditions in each category. Some of the examples of subcategories are as follows:

- Data in storage protection system subcategory
- External information systems directory subcategory
- Detection systems alerts subcategory

There are particular guidelines, standards and practices to e-government essential infrastructure. It demonstrates processes necessary for the achievement outcomes related to every category, they are referred to as Instruction reference. It has a vivid representation in the framework nucleus. They are based on advanced guide which are highly considered in the framework development process.

The framework nucleus works simultaneously and consistently to structure an effective way of addressing security risk.

The Framework is flexible, making room for government, agencies and departments to utilise subcategories and instruction references that are resourceful and may facilitate the management of security challenges.

The management of e-government security processes which includes legal, institutional, regulatory requirements, business and service requirements, and governmental constraints directs the choice of some actions in the creation of a Profile. Personal information is seen as an aspect of data referred to in the categories while considering security risks and also defence mechanisms (NIST, 2014a, p.7).

The purpose of this framework to provide a proactive security for e-government services some of which are listed in Section 5.5, principally through the Identification of threats, Protection or defence of the system against threats, Detection of risks factors, Respond or counter the risk and to Restore the system to normal operations. Table 5.1 shows categorization of actions under a given function to achieve a target secured outcome. This categorization of actions will help the organisation to effectively review their processes by checking the list to know if they are on track and make necessary adjustments.

Table 5:15 Framework's functions and categories

Function ID	Function	Category
ID	IDENTIFY	- Management of Assets - Environmental conditions of the business - Issues of Governance - Risk measurement - Strategies in managing security risk
PT	PROTECT	- Access control measures - User sensitization and Training - Data security - Security of Processes - System Maintenance - Defensive Technology
DT	DETECT	- Freaks and Incidents - Constant Security Checking - Detection Techniques
RD	RESPOND	- Plan for Counter Measures - Reporting - Investigation
RT	RESTORE	- Plan to Restore - Advancement - Reporting

Identify: The identify function basically conducts a risk assessment to identify vulnerabilities in the system; there could be several unknown vulnerabilities in a system. There must be proper process of identifying these system vulnerabilities, so that a solution can be proffered. Government must have an understanding on the ways of administering or managing security threats to critical infrastructure, resources and sensitive data. Actions taken under the Identify function are quite introductory in the overall successful utilization of the framework. Getting to know

the way things work with the critical asset that facilitates essential functions and associated threats to e-government security. Resources that maintain essential functions and the associated security risks allow a government to articulate its endeavours, in consonance with its security strategies and service requirements (NIST, 2014a, p.8). Some of the examples of outcome categories in this function are:

- Risk assessment/measurement
- Management of Assets
- Environmental conditions of the business
- Issues of Governance
- Strategies in managing security risk

Defend (Protect): After identifying potential risk to the organisation, there will be a defence or protection mechanism in place, each threat type must be individually planned for. Its aim is to supported and protected in order to bring under control the severity of any possible security incidence (NIST, 2014a, p.8). Some of the attributes of the defend function are:

- Access restriction measures
- User sensitization and Training
- Data Security
- Information Protection Processes and Procedures;
- System Maintenance

Detect: The detect function is relevant in situations where an incident occurs, the source of the fault or compromise must be quickly detected. The detect function seeks to carry out a design and implementation of a system that will identify any security incident within the e-government platform. It will ensure swift detection of security incidences (NIST, 2014a, p.8). Some of the examples are:

- Irregularity and Incidence
- Constant Security Checking
- Detection Processes.

Act in Response (Respond): The system is not expected to fail irrespective of underlying errors, therefore the source a compromise has been detect there must be strategy for correction of such errors. There will a design and process of implementing suitable measures needed to respond to any security occurrences and processes that may reduce the severity of impending security incidence (NIST, 2014a, p.8). Some of the examples are:

- Response Strategy
- Communications Strategy
- Investigation
- Mitigation Strategy

Restore (Recover): This function ensures that the time lag for processes to resume after any incidence is negligible; often times users may get to know about an incidence after management communicates it. Restore or recover function is to design and implement suitable measures that will ensure buoyancy and also reinstate whatever services that were compromised during the security incidence. It supports swift recovery to regular activities thereby reducing the severity of security incidence. Some of the examples are:

- Recovery strategy
- Improvement strategy
- Communications strategy (NIST, 2014a, p.8).

The nucleus of this framework which is the Identification of threats, protection or defence of the system against threats, detection of risks factors, respond or counter the risk and restore the system to normal operations are in consonance with the Nigerian National Information Systems and Network Security Standards and Guideline empowered by the NITDA Act of 2013.

Framework Implementation Levels

The Framework Implementation Levels give a background to how a government organisation views security threats and the modalities for managing such threats. The Levels are Partial (Level One) to Adaptive (Level Four) which illustrate a growing

level of intransigence and sophistication in the management of security threats characterized by service requirements and are incorporated into the government's general security management plan (NIST, 2014a, p.9).

Security management strategy involves several areas of e-government security, particularly the aspect of data privacy. The process of selecting a level takes into consideration present security management procedures, risk conditions, legal considerations, services requirements as well as limitations (NIST, 2014a, p.9).

Government will establish the required level, making sure the particular level measures up to the set goals, and reduces threat to e-government critical assets to acceptable levels (NIST, 2014a, p.9).

Government agencies initiating e-government strategies have to think about taking advantage of established guidelines or sources, existing e-government maturity models in formulating required levels.

Organisations selected as Level One (Partial) are persuaded to move to Level Two or even higher, Levels may not necessarily signify maturity levels. Development to a high Level is advised in a situation where it will help in reducing security threats and also guarantee capital reduction. The success of a framework is mostly consequent upon accomplishment of the expected result outlined in the government's objective Profile(s) but not dependent entirely on the strength of a particular level (NIST, 2014a, p.9).

Level One: Partial

Threat Management Process

Here the government security threat management processes are mostly improperly organised, also threats are handled in a makeshift and somewhat impulsive way (NIST, 2014a, p.10).

Integrated Threat Management Programme

There seem to be an inadequate knowledge of security risks throughout the levels of government and the entire government's security mitigation plan. The

government will implement a program to handle security threats in an asymmetrical, step-by-step basis, because of diverse knowledge acquired from external resources. Government sometimes are unable to carry out actions that will enhance the even distribution of information related to security risk within the government departments (NIST, 2014a, p.10).

External Contribution

There is a seeming lack of harmonization or cooperation among the various organs of government (NIST, 2014a, p.10).

Level Two: Risk Informed

Threat Management Process

Threat management processes are employed by stakeholders though not accepted as a standard government policy that will be binding on all the organs of government.

Integrated Threat Management Programme

There seem to be an adequate knowledge of threat to security across government levels but the government's method of handling security situations is yet to be outlined. Those aware of the risk, stakeholders-recognised procedures are designed so that members of staff will have sufficient means to carry out the e-government security responsibilities. Security information here is shared within the government organisation on an unstructured and non-formalized manner (NIST, 2014a, p.10).

External Contribution

The particular government entity is aware of its responsibility amongst the greater network, though yet to outline these functions and communicate it to stakeholders both internal and external.

Level 3: Repeatable

Threat Management Process

The manner with which government manages its security risk is properly formulated and articulated as a policy. The government security processes are often restructured relevant to some of the threat management practices or changes in service needs as well as technological advancements.

Integrated Threat Management Programme

A general government way of managing threats to security, security-based strategies are outlined according to regulations and implemented as planned. Reliable techniques are also established to successfully act in response to any security incidence. Trained staff has been given adequate tools to carry out designated assignments based on their skills set.

External Contribution

The government appreciates its strategic relationship with stakeholders and get relevant updates that enhance cross-cutting cooperation in relation to how to swiftly deal with security threats within government.

Level 4: Adaptive

Threat Management Process

The government tailors its information security activities according to knowledge derived from past incidences or predictions in line with trends in the cyber security landscape. With strict adherence relevant security standards and the implementation of security technologies and principles, government will be able to respond to e-government threats successfully.

Integrated Threat Management Programme

General government way of handling security threats which employs security-aware principles in addressing probable security incidence. E-government security related threats management are carried out in accordance with its understanding of

standard bureaucratic cultures which grows from its knowledge prior events, records of in other data sources, and growing knowledge of events across external networks (NIST, 2014a, p.11).

External Contribution

The particular government handles security threats and dynamically distribute the message amongst participating stakeholders with the aim of ensuring correct up to date information gets across to relevant endpoints before any devastating security incidence (NIST, 2014a, p.11).

Framework Outline

Framework Outline comprises functions, categories and subcategories alongside other service needs, government assets and security risk tolerance measures.

Profile allows government create a strategy for minimizing security threats that are associated with e-government services. Due to the intricacy of many government services, government could decide to keep different profiles, associating them with specific mechanisms while acknowledging their respective needs (NIST, 2014a, p.11).

Framework Profiles can be used to illustrate the present state or the required target state of specific security activities. The Current Profile indicates the security situation as it is at any given point in time, it gives a real-time report.

The goal of a Profile is to demonstrate actions necessary to achieve basic security threat management objectives (NIST, 2014a, p.11).

Profile evaluation could be either Current or Target Profiles for instance, which has the capacity to security expose breaches as one of the major objectives of a security risk management plan.

Service needs and risk management processes are responsible for the priority given to mitigation of security breaches (NIST, 2014a, p.11).

The implementation process of the framework has to be properly harmonised to allow for an easy information and decision-making process. A description of an organisational flow process of government is as follows:

- The Executive level
- The Business and Process level
- The Implementation and Operations level

At the first level which is the executive level is where the priority services, system assets and organisational risk tolerant mechanisms are communicated to the next level known as the business or process level. The process level now accepts the communication as input to the risk management process in collaboration with the implementation level which will communicate required services used in creating a profile. The implementation level also communicates the profile performance update to the business level. At the business level an impact evaluation is conducted based on the information received, the result is then transmitted to the executive level for another evaluation before the final report of the impact of the threat will be published to all in the organisation (NIST, 2014a, p.12).

The executive level communicates the service priorities, available resources, and overall risk tolerance to the business/process level. The business/process level uses the information as input into the risk management process, and then collaborates with the implementation/operations level to communicate service needs and create a Profile (NIST, 2014a).

The implementation/operations level communicates the Profile performance update to the business/process level. The business/process level uses this information to perform an impact assessment. Business/process level management reports the outcomes of that impact assessment to the executive level to inform the organisation’s overall risk management process and to the implementation/operations level for awareness of business impact (NIST, 2014a).

How the Nigerian Government can apply this Framework

The NIST cyber security framework is very flexible for adaptation to any country, and has great resources in terms of updates and quick response to changes in the management of cyber security risk. The Nigeria government may use this framework as a major component of its strategic e-government security implementation plan for the identification, assessment and management of security threats. The recommendation of this framework is not to replace existing procedures or processes, but it is to identify imminent breaches in present security risk management plan in order to provide a credible way out.

Using this e-government security framework, the government or its agencies will be properly guided to agree on fundamental actions that may be crucial to cost savings and aid in budgetary allocations of funds so as to take full advantage of the impact of government investment in e-services.

The framework was built to enhance current services or e-government security processes. It could provide the basis for a novel e-government security paradigm or methods for the advancement of current security plans.

It however presents concerns and processes for evaluating the implications of privacy within e-government. There are diverse ways by which the government and its agencies can apply this framework. The NIST cyber security framework has been an initiative of a great science and technology institution founded in 1901 by the United States government; its proven research background makes it acceptable and easily assimilated by Nigerian policy makers, as the country tends to rely greatly upon the legacies of the USA from whence it adopted its presidential system of government in October 1975 (Teniola, 2014).

Fundamental Reassessment of E-Government Security Practices

The framework could be employed to evaluate a government's current security plans and the ones outlined in the framework nucleus. In course of the creation of a Current Profile, government may check the level to which they are realizing the results depicted in the Nucleus Categories and Subcategories, associated with the

five high-level Functions: Identify, Protect, Detect, Respond and Recover (NIST, 2014a, p.13).

A government can discover its progress towards achieving expected outcomes, therefore implementing security that is well proportionate to the identified risk. On the other hand, a government organisation may consider improving the security in accordance with the identified needs (NIST, 2014a).

The government department may utilize the knowledge gained to develop a plan to brace current security practices thereby minimizing e-government security risk (NIST, 2014a, p.13).

Establishing or Improving an E-Government Security Programme

The various stages of actions illustrated below are ways in which government could utilize the framework to build a novel security plan or develop upon an existing security programme. It is recommended that the following steps be adhered to for constant improvement on the security of the e-government (NIST, 2014a, p.14).

Stage one: Priority and Scope

The government will identify business or service expectations and priorities. Based on these known objectives, government will then formulate a strategy about security operations and establish what is required to provide adequate support for selected services. This framework is flexible it could be tailored to work with several types of services within the e-government system (NIST, 2014a, p.14).

Stage two: Orient

After establishing the magnitude and scale of the security programme for the services required, the government will further identify interrelated schemes and resources, statutory requirements and other risk related approaches. The government will also carry out vulnerability assessments to determine threats to systems resources (NIST, 2014a, p.14).

Stage three: Create a present state outline

Government will build up an outline that represents the present state of things by indicating the outcomes of either the Category or Subcategory of the Framework Nucleus that is been presently actualized (NIST, 2014a, p.14).

Stage four: Carry out a risk level assessment

This assessment could be directed by the government's overall threat management process or prior risk assessment activities. The government evaluates the conditions of operation so as to identify the probability of a security incidence as well as the effect that the incidence could bring to the government. It is therefore imperative that government endeavour to integrate potential risks or vulnerability data that will support dynamism of the chances and impact of security incidences (NIST, 2014a, p.14).

Stage five: Create an objective outline (Target Outline)

The government makes a Target Outline that centres on the evaluation of the framework categories and subcategories demonstrating the governments expected security outcomes. Government organisations may also implement their own supplementary categories and subcategories to explain for the unique associated risks. Government may also give consideration to authorities and needs of external stakeholders like customers or business partners in making an objective outline (NIST, 2014a, p.14).

Step six: Evaluate, Establish and Prioritize Breaches

Government evaluates the current Outline and the Target Outline to determine breaches. After which it builds a structured action plan to deal with those breaches that bothers on service drivers, cost and benefit analysis and the comprehension of risk to accomplish the outcomes within the Target Outline. The government then identifies resources needed to tackle the breaches. Making use of outlines in this way makes the government more informed in its decision-making process about

security activities, supporting threat management and enabling the government departments to carry out cost-effective, targeted development (NIST, 2014a, p.14).

Step seven: Implement Action Plan

The government initiates plans to carry out as it relates to security breaches, where any breach is noticed or identified; it will then monitor its present security practices compared to the Target Outline. Furthermore, the framework identifies sample Instruction References about the categories and subcategories, however government have to determine what standards, procedures, guidelines as well as those that may peculiar to sectors, work perfectly for their requirements (NIST, 2014a, p.14).

The government could repeat the actions as often as necessary to continually evaluate and enhance security. For example, government could discover that more regular repetition of the Orient stage increases the quality of risk evaluations. Moreover, government can measure progress through repetitious updates to the current Outline, subsequent comparison of the Current Outline to the Target Outline. Government can as well use the method to support their security programme with the required framework implementation level (NIST, 2014a, p.15).

Communicating Security Requirements amongst Stakeholders

The framework presents a general mode of communicating requirements amongst mutually dependent stakeholders who are saddled with the task of delivering essential infrastructure services, such as:

- The government could use a target outline in communicating security threat management requests to external service providers (In this case, it could be some cloud services providers).
- The government can communicate its security status via a current outline to report outcomes or even to draw comparison with expected outcomes.
- A critical infrastructure operator that has been able to establish that a very important stakeholder, who depends greatly on the infrastructure, could employ a target profile to communicate vital categories and subcategories.

- A vital infrastructure sector can set up a Target Profile that could be employed amongst other components as a first standard outline to develop a novel Target Outline.

To Identify Opportunities for New or Modified Instruction References

The Framework can be used to identify opportunities for new or revised standards, guidelines, or practices where additional Instruction References would help organisations address emerging needs. An organisation implementing a given Subcategory, or developing a new Subcategory, may find out that there are few Instruction References, if any, for a related activity. To attend to that need, the government might collaborate with technology leaders or standard organisations to draw up, develop, and put together standards, guidelines, or practices (NIST, 2014a, p.15).

Methodology to Protect Privacy of Citizens

This section explains the methodology for addressing individual privacy inferences that could affect security operations. This methodology was proposed to be a universal procedure due to the fact that privacy considerations varies from sector to sector across a given period of time, so government will deal with concerns of proficiency.

However, not every activity in a security programme may require these considerations. Novel privacy standards and added best practices are required to maintain better technological adoptions in this regard. Privacy concerns could come up when there is collection, processing or disclosure of private information in connection with government's security plans (NIST, 2014a, p.15).

Instances of practices that bear privacy considerations includes: security practices that end up in the excessive collection or excessive retention of private information; disclosing or usage of private information not related to security practices; security mitigation practices that end up causing denial of service or related potential undesirable effects, as well as actions like incident detection efforts that can affect people's liberty to associate or communicate freely (NIST, 2014a).

Government and its agents are saddled with the duty to defend the privacy of citizens in respect of security activities they engage in. Accordingly, government and its agents that operate essential infrastructure have to ensure that there are laid down procedures to maintain security compliance practices with appropriate privacy policies and regulations within the confines of the law.

In addressing privacy concerns, government have to ensure that at the appropriate instance, security policies should integrate fundamental privacy values like: data disclosure, retention of materials containing private information of the security incident; place restrictions on security practices on any material used exclusively for security programmes; ensure transparent transactions on key security activities; permission must be sought and adequate remedy offered in situations where there are adversities as a result of the utilization of private information in security programmes; ensure integrity, accountability, availability and non-repudiation (NIST, 2014a, p.16).

5:1 Framework Nucleus

FUNCTION	CATEGORY	SUBCATEGORY	Information References
IDENTIFY	**Management of Assets** The human resources, systems, data and services that make it possible for government to accomplish business goals are identified and administered consistently with corresponding values to set out objectives and organisational risk plan.	- Outline physical components and systems within the establishment - Outlines software applications and related platforms in the establishment - Plan internal methods transmitting data within the establishment - Make an inventory of external information systems - Allocate priority to resources according to category and value.	(NIST, 2014a, p.20)
	Environmental conditions for business Government and stakeholders actions are established and categorised; this information is employed for the determination of security responsibilities as well as threat management assessment.	- Government's responsibility in the provision of resources are spelt out - The position of government in the provision essential infrastructure alongside its speciality is spelt out and reported accordingly - Different stages of activities are spelt out according its level of priority - Essential actions and dependencies for the provision of essential services are outlined	(NIST, 2014a, p.20)

	Governance Outline the processes and procedures for governing requirements for government's regulations, laws, security, environment and operations.	- Establish government information security policies - Info security responsibilities are harmonized with other task among internal and external partners - Establish Legal and regulatory frameworks related to cyber security - Governance issues and risk management processes address e-government-security risks	(NIST, 2014a, p.21)
	Risk Measurement The government understands the security risk to government operational resources and personnel.	- Vulnerabilities of assets verified and reported - Check online forums and other sources for vulnerabilities and threats - Internal and external threats are verified and reported - Potential effects on businesses and possibilities are verified and used to determine risk - Risk response techniques are established and categorised	(NIST, 2014a, p.22)
	Strategies for the management of risk Establish government's priorities, limitations, risk tolerances, and suppositions and use to shore up operational risk assessments	- Stakeholders should agree on risk management procedures - Risk tolerant indicators are well identified and outlined - The identification of risk tolerant indicators are determined by its impact in essential infrastructure and sector-specific risk evaluation	(NIST, 2014a, p.23)

PROTECT	**Access Control Measures** Access to information and transactions are restricted to only those authorized to have access in line with access policies which could be based on hierarchical distribution in the organisation.	- Identities and credentials are managed for authorized devices and users - Secure physical access to assets and information from unauthorized persons - Controlling of virtual access - Granting of access are highly restricted, introducing least privilege and duty separation policies - Ensure the protection of network integrity	(NIST, 2014a, p.23)
	User Sensitization and Training Government officials and consultants are given security awareness trainings to carry out security-related functions while observing requisite security policies and regulations.	- Sensitize all users of e-government - Privileged users should be aware of their respective privileges - Define the roles and privileges of external stakeholders - Define the privileges of top officials to avoid misunderstanding - Define the privileges and responsibilities of human security personnel as well as other IT security personnel	(NIST, 2014a, p.24)

	Data Security Services and system resources administered according to the prescribed plan in the government's risk to ensure the protection of data integrity, confidentiality, availability and non-repudiation.	- Protect data in storage - Protect data in transit - Sufficient capability to guarantee 24hours availability of assets - Implementation of mechanisms to protect against data leakages - Mechanism for checking integrity are utilized to determine systems integrity	(NIST, 2014a, p.25)

	Security of Processes Security policies on scope, responsibilities and the harmonization of government establishments, processes and dealings are sustained and employed to manage security of systems resources	- Create and maintain a standard configuration of technical systems - Implement a system development life cycle - Ensure adequate controls over configuration changes - Carry out and maintain systems backups and test regularly - Comply with policies and regulations concerning the physical operational environment for government resources - Security techniques are regularly improved upon - Sharing of security technologies with relevant stakeholders - Adequately monitor plans on incident response - Adequately monitor plans on business continuity - Adequately monitor plans on disaster recovery Test plan on the response and recovery mechanism - Plan for the implementation of a vulnerability assessment and control	(NIST, 2014a, p.26)
	System Maintenance: Repair and maintain technical controls and e-government system.	- Maintain systems resources , log it accordingly in line with standard practice - Conduct remote maintenance of system resources without exposing access to unauthorized persons	(NIST, 2014a, p.28)

	Defensive Technology Managing security mechanisms and ensuring it remains resilient in accordance with relevant policies and agreements.	- Records logging and auditing are done with strict compliance to relevant policies and agreements. - All secondary storage devices are kept in safe conditions ensuring all access control policies are observed. - Restriction of access to systems resources, integrating the theory of least functionality - Adequate protection of every communication devices on the network.	(NIST, 2014a, p.29)
DETECT	**Freaks and Events** Unusual activities are identified swiftly and possible effects are established	- Basic standard for network operations and system transactions are determined - Security breaches detected are screened to understand possible target of attack and methods employed - Event data are aggregated and correlated from multiple sources and sensors - Impact of events is determined - Incident alert thresholds are established	(NIST, 2014a, p.30)

	Security Continuous Monitoring The system resources and services are monitored at regularly intervals to identify security incidents so as to offer efficient security measures.	- Monitor the network infrastructure to identify potential e-government security incidences. - Monitor the physical perimeter to identify possible e-government security threats - Monitor activities of personnel to identify possible security breaches - Screen to identify malicious source codes - Monitor to identify malicious mobile codes - Monitor activities of third party agents like consultants and suppliers for identify possible security breaches - Monitor the performance of unauthorized users, cables, equipment and computer programs - Perform vulnerability scanning	(NIST, 2014a, p.30)
	Detection Processes The mechanisms for detection of threats are constantly checked to make sure it is performing optimally	- Methods of threat for detection are clearly stated to make sure that there is accountability - Detection activities must be compliant with requisite policies - Test detection techniques - Information about detection of threats are sent to relevant stakeholders - The techniques for detection are regularly improved	(NIST, 2014a, p.31)

RESPONDS	**Response Planning** Response techniques carried out and sustained to make sure that there a swift response to identified threats.	- Strategies for response are usually carried out during an attack or after it.	(NIST, 2014a, p.33)
	Communications Strategies for response are adequately outlined for stakeholders and expect assistance from law enforcement agents where necessary.	- Personnel know their roles and order of operations when a response is needed - Events are reported consistent with established criteria - Information is shared consistent with response plans - Coordination with stakeholders occurs consistent with response plans - Voluntary information sharing occurs with external stakeholders to achieve broader e-government security situational awareness	(NIST, 2014a, p.33)
	Analysis Proper analysis is carried out to make sure a swift response is provided in times of system recovery	- Investigate alerts provided by detection systems - Understand the effect of the incident - Conduct forensic analysis to identify source of threat	(NIST, 2014a, p.33)

	Mitigation Carry out actions that avoid escalation of a breach, ease the effect on service output and eliminate future occurrence.	- Incidents are contained - Mitigate security threats - New threats are contained, if not immediately possible it acknowledged as acceptable risk factor	(NIST, 2014a, p.34)
	Improvements Government's response activities are improved by incorporating lessons learned from current and previous detection/response activities.	- Plans for response also take into consideration lessons learned - Techniques for response are usually updated	(NIST, 2014a, p.34)
RESTORE (RECOVER)	**Recovery Planning** Restoration techniques carried out and sustained to make sure that there a swift response to identified threats	- Strategies for response are usually carried out during an attack or after it.	(NIST, 2014a, p.34)

	Improvements Recovery planning and processes are improved by incorporating lessons learned into future activities.	- Plans for recovery also take into consideration lessons learned - Strategies for recovery are regularly updated	(NIST, 2014a, p.35)
	Communications Restoration procedures are carried out alongside important stakeholders' service providers, customers and suppliers.	- Control the image of the establishment through professional PR services - Manage the reputation of the establishment after an incidence has occurred	(NIST, 2014a, p.35)

Modalities are put in place to identify and deal with the privacy concerns that has to do with access control mechanisms which may include collection of data, disclosure of information, or the use of private information awareness and training measures. Policies that will tackle privacy concerns will be made available to IT security practitioners as well as other stakeholders like the services providers or consultants so that they can be abreast with all relevant rules in the policy. There must be a planned course of action to carry out a policy review on the identification of potential breaches, security monitoring and response mechanisms, as well as data sharing and mitigation plans.

There is a procedure for the assessment and determination of how and to what extent private information is communicated to authorized recipients external to the establishment as part of security data sharing practice.

Summary

It can be deduced from the above that the essentials of a security plan comprises the following: access control, security sensitization and training, auditing and accountability, security appraisal and authorization, identification and authentication, contingency planning, incident response, system maintenance, configuration management, physical and environmental defence mechanism, planning, security of personnel, evaluation of risk, acquisition of systems, protection of communication links, data integrity and management of programs.

Proper understanding of existing security standard practices helps to foster better planning of new security architecture or a security framework. After looking at compliance issues relating to standards, policies, guidelines in tackling e-government threats and vulnerabilities, a framework was defined, pointing out its significance in addressing security problems. Defining a framework and its requirements or fundamentals necessitated the assessment of existing frameworks, it was however observed that these frameworks were suitable in a few situations but were largely limited in scope.

The proposed framework advanced an approach to mitigate security threats associated with e-government which consists of three different elements: the framework nucleus, the framework implementation levels, and the framework outline. The entire framework components strengthen the link between e-government security drivers and e-government security strategies.

Strategic Framework for a Secure E-Government in Nigeria

Introduction

This chapter presents the proposed framework composition and the framework components as a vital component of any e-government strategy. An explanation of how the framework was evaluated and the responses of the expert opinions that were sought are all captured in this chapter. A detailed analysis on the respective evaluation criterion was itemised and reported accordingly. Since it was imperative to point out that the critical contemporary e-government infrastructures with its sophisticated technologies are built over 'traditional' networks that are relatively insufficient in many aspects. These systems often require dependability, fault tolerance, reliability, security, survivability or some other characteristics that were not evidently foreseen when they were initially built, and they were integrated as an afterthought (Al-Kuwaiti & Kyriakopoulos, 2006).

Significance of a Strategic Framework for a secure E-government

One of the primary purposes of this work was to put together a strategic framework for secure e-government in Nigeria. The framework will serve as a standard abstraction of an e-government security strategy. In spite of its straightforward approach, as will be illustrated, an e-government security strategy framework seems to be absent in most available national e-government strategies, though maybe not to the extent that is presented in the study.

Putting together an e-government security strategy framework may bring about certain advantages to the government in Nigeria. Presently, there are efforts by the Nigerian government to implement a broad, well-structured framework or implementation approach that will be more beneficial to the government in terms of time savings and funding (Dawes, 2008).

Pictorial representations are much easier to understand than several pages of text. An e-government security strategy framework is not expected to substitute the complete text of an e-government strategy but rather to enhance it; it should

provide a more viable option. It is a graphical representation so it provides such information at a glance, particularly if it is professionally presented to highlight the key concepts.

It appears to be a very valuable tool for top government executives at the final decision-making levels. Well suited for political office holders who may not be technical experts in the field, for easier understanding, pictorial or graphical presentations are much simpler compared to long texts. Moreover, a strategic framework provides a simpler but complete conception as to what the e-government security goals are. It basically displays the focus or the security perspective of the e-government implementation.

The framework is crucial mostly during stakeholders meetings on e-government projects. When there is a necessity to refer to the security strategy, in that case it may be more reasonable to look through the framework for quick demonstration of what the strategy is. If there is more information that may be needed, the comprehensive strategy will be sought.

As an all-inclusive concept, the strategic framework demonstrates the way various fundamental components work mutually to achieve a purpose. It explains how every section relates to another. It ensures that project plans and projections are achieved with minimal deviations or disagreements.

Also considering that it is visual, the strategic framework of e-government security must not be seen to be jumbled or complex. It must be very straightforward and also easy to understand. Otherwise it will be counterproductive, and would have lost its essence. If you concentrate on making the framework very complex it will lose its significance as well as usability.

Although it is crucial to emphasize the key features of the security framework, a strategy framework document is expected to come in a very simplified language due to its strategic importance and necessity in the accomplishment of e-government security goals.

E-government security strategic frameworks have a comparatively long duration to accomplish their set goals due to their characteristic broad-scope. Therefore to stay with this scope, the framework will have to be amenable to potential changes within the system. This field of technology is still evolving and revolutionary; therefore there will be frequent need to make adjustments based on certain social, leadership and environmental conditions. So the framework should not be adversely affected by changes in external conditions; it must be flexible and adjustable accordingly (Chen et al., 2006). One of the ways to achieve strategy flexibility is to ensure that its components are technology-neutral.

The study planned to develop a general framework but considering some of the issues listed below, it was considered impracticable, at least not within the resources made available for the duration of this research, and it appeared that one size will not fit all. Several identifiable diversities across nations of the world may be found. Countries are divergent in one or more ways as highlighted in the list below:

1. Culture and tradition
2. Legal and regulatory structure
3. Economic system
4. Infrastructural and technological development
5. Technology and internet penetration
6. Availability of skills and human resources
7. Political Structure
8. Educational system
9. Citizens identification system

Al-ahmad et al. (2008) in their research 'An extended framework for e-government security' highlighted several important security requirements in a framework. However, they left out some underlying issues necessary in ensuring e-government security. For example, user identification is a major factor in e-government security

but was not considered in their framework, the user's credentials must be verified before granting access to critical government services in line with relevant policies, otherwise the technology could be considered to have failed (Sanchez-Martinez et al., 2008).

The European Information Society, EURIM Personal Identity and Data sharing Working Group reported in April 2005 thus:

> "Advances in computing, particularly in networking and security, are making it possible to reduce identity theft through secure data sharing, but new technologies often raise more questions than they answer: questions of national identity and the relationship between citizen and the state, about civil liberties, data protection and relationships with other nations and commercial organisations, about citizens owning their data and the government being free to access it in the national interest. These factors must be seen to operate in balance if secure e-government is to be delivered in an acceptable way for all stakeholders" (European Information Society Group, 2005, p.1)

Consequent upon the above assertion, citizen profiling is critical; unique identification is equally essential. Every e-government security framework is expected to satisfy the following conditions: Authentication, Authorization, Non-Repudiation, Confidentiality, Integrity and Availability (Lean et al., 2009).

Registration and Authentication Strategy

This develops upon the e-government security policy that situates the e-government security requirements, and it particularly deals with those security requests related to the provision of registration and authentication services to support access to e-government services.

Registration

Registration is a process where users obtain credentials like usernames or digital certificates for the purposes of authentication. It could demand that the client

should show some sought of verifiable evidence for identification, it could be a national identity, citizen's certificate or work id (Health & Social Care Information Centre, 2002).

Authentication

Authentication is a way of verifying the electronic identity of a potential client with the aim of confirming or rejecting the client based on credentials obtained during an earlier registration. The verification could be several methods, password or biometric methods (Health & Social Care Information Centre, 2002). Users are expected to be authenticated electronically at every point of access to the e-government platform (Asogwa, 2013). This process is expected to provide for a secure login that will be mapped to the citizen's profile. Therefore, the first stage will be registration; consequent upon the fact that in Nigeria there is no unique identification like the National Insurance Number as obtainable in the UK or the Social Security Number as in the USA. There are also no post codes or zip codes to map citizens' addresses. There are no definite ways of tracing people's residential contact addresses due to the traditional settlement patterns whereby about 48% of residents live in rural and semi-urban areas (Afon & Faniran, 2013). The issue of identity authentication is critical consideration for those providing e-government services. It could be either by those in the public or the private sectors that are saddled with the responsibilities of providing e-government services, they could be regulators, auditors, controllers of public assets, contractors, service providers that regulatory bodies responsible for the proper audit and control of public assets and information, and the suppliers and service providers that manage these services for the government.

Description of Risk Associated to User Authentication and Possible Countermeasures

Authentication depends on the substantiation of one or more factors such as: something the applicant knows, a secret such as a password, something the applicant has, such as a token and something the applicant is, such as biometric or

set of other attributes like age, colour of eyes etc. Once a person is authenticated it means the claim(s) are valid, the service provided cannot afford to make mistakes in this regard, as any errors may be costly particularly in issues that requires high degree of protection like financial transactions.

Table 6:16 Risk associated with e-government user authentication and countermeasures (adapted from Health & Social Care Information Centre, 2002)

S/N	Risk associated to authentication in e-government	Plausible Countermeasures
1	False real-world identification: A user could acquire a credential associated to a false real-world identity.	Plausible countermeasures to ascertain that there is an actual identity before issuing credentials are: - Verifying the credentials presented with citizens data stored in the database - Verifying through comparison with original documents
2	Fictitious Information: Forged information may be recorded against a real identity, thus making it credible.	Plausible ways to verify that personal information provided during the registration are correct are as follows: - Cross-check information provided by an applicant with records in the government's legitimate citizens record - Ask the applicant to declare that the information provided is adequate and if it is proven to be the contrary, he will face penalties according to the laws - Request for attestation of applicants by reputable persons or organisations.
3	Identity theft: A valid identity might be stolen during registration.	Plausible ways to ascertain that guarantee that the credential is issued to the real owner of the identity are as follows: - Probing the originality of documents during the registration process - Requesting that applicants provide answers to fundamental questions as a way verifying true identity - Request for an attestation or reference letter from a person of high repute in society - Sending correspondence to the supposed applicant at the address provided in the registration forms
4	Disclosing or Interfering with secret authentication information like the Personal Identity Number or One-Time Password.	Plausible ways of reducing the risk associated to secret authentication information from being interception or internal or unintentional disclosure are: - Make sure any information to be transmitted are secure, ensuring it passes through the process of encryption - Let the transmission process be done bit by bit - The use of a more dynamic question during identity verification may be more reliable than the static questions like maiden name. - Introducing a contract agreement that requires the applicant not to disclose his secret authentication codes

5	Keeping the secret authentication information in an unsecured location: Secret information may be kept in an unsecured storage device or location perhaps on a computer in a general office. It could be a private signing key used to perform cryptographic functions or a secret code inputted into an online register stored in a cache server.	Some of the countermeasures against this type of security risk may have to be technology-specific, which are the following: - To ensure that secret data are not retained in an unsecured device, they should rather be saved in a wholly reliable token like a smart card that could carry out signature functions - To ensure that any secret information is suitably managed and rid of when necessary.
6	The continuous use of compromised credential	Plausible countermeasures against use of a compromised credential are: - To enable and encourage applicants and the RP to disclose suspected breach - Giving fixed term limit to credentials provided - To enable service RP to verify the legality of a credential at the particular instance by referencing a credential revocation list - To enable RP to get positive proof of the validity of a credential at time of use, through an approved process.
7	The use of a credential subsequent to a substantive change in status:	Plausible actions to avoid the usage of a credential subsequent to a substantive change in status are: - Agreeing to oblige clients to inform the authorities of any changes in their status
8	Inappropriate withdrawal of credential may be due to fictitious or malevolent information of change in status or compromise of credential.	Plausible ways of reducing the risk associated to, or problems as a result of improper withdrawal of a credential are as follows: - The registration authorities should have access to the verification details to offer some measure of assurances that the individual calling to report a compromise or a change of status is authentic.
9	Using the credential issued to commit fraud:	Plausible ways to avoid the risk associated to unnecessary usage of credentials are as follows: - To statutorily oblige the credential owner to use it for on what it was meant for - The usage of dynamic information to verify that a credential is still possessed by correct person - The use of biometric data verification to make sure that the credential is still possessed the correct client - To ensure that services provided are in accordance within the limits of agreement and use of the given credential.

The Need for an Identity and the Process of Identification

The process of identification is a dynamic compilation of every attribute associated with a definite entity, usually by a citizen, although the idea could be extended to incorporate enterprises or objects. It seems universally acceptable that an identity is what gives permission to individuals to be identifiable. This however, makes identification or identity management a major factor in several financial, public and governmental dealings. The capacity to connect information to its rightful possessor efficiently and in secure way is very critical (Collings, 2008).

Therefore technological means, systems for managing identities was to classify, allocate, spell out ranks of authority, allot responsibilities to and direct the identity elements associated to special individuals like members of staff, clients as well as citizens. Identity is very significant but almost being relegated because of the very intricate advancement in technology in today's society. It is because of the resurgence of ID card systems and the increase in Internet and electronic scam that has resulted in the initiation and appreciation of the actual issues that highlight identity and its effects on society (Collings, 2008).

There is a need for a smart and simple approach by which citizens in Nigeria could be uniquely identified in the near future because efforts in the past to issue Citizens National identity cards have failed. Referring to an article published on the 2nd of July 2008 in a Lagos-based newspaper *ThisDay*, 'Nigeria's identity card project has apparently been "riddled with fraud." Irregularities associated with the identity cards included multiple "false documentation," applications made by people that were not up to the statutory age of eighteen and so many mistakes on the cards' (Research Directorate of Immigration and Refugee Board of Canada, 2014). On 10th August 2006, *This Day Newspaper* reported that over seven million national identity cards were cancelled because of these irregularities. Another article published by the Nigerian daily newspaper *Business Day* on 16th October 2007, wrote that the national Identity card were unverifiable due to absence of unique codes for

authentication (Research Directorate of Immigration and Refugee Board of Canada, 2014).

Proposed E-Government Security Framework

The Framework is intended to advance the rapid adoption of practices that will guarantee e-government security. It seeks to offer a flexible, repeatable and economical way of implementing e-government security.

The framework will provide a major direction to government with the aim of growing the confidence of customers. Furthermore, it will make sure that security techniques adopted are in accordance with information security policies. The framework components possess the capabilities to identify threats and attacks to e-government services.

There is a mechanism that will be able to analyse and report risk; it is a software application integrated into the system. The proposed framework will integrate a technique to prompt incidence reporting, while the secure communication provided by PKI based on SSL/TLS protocols will ensure confidentiality; non-repudiation can be described by certificate passing plus the integrity check from the message authentication.

The framework considers every aspect of e-government security: the people, the process and the technologies. The framework was built strategically to function in accordance with relevant regulatory and legal frameworks, such as the Nigeria Cybercrime Act, 2015 which was recently passed into law. The provision of the Act is to

> "ensure an efficient, integrated and comprehensive institutional, legal and regulatory framework for the prevention, prohibition, prosecution, detection and punishment of cybercrimes in Nigeria. The act is also to protect all critical national information infrastructure and promote cyber security, protect computer systems and networks, computer programs and data, electronic

> communications, intellectual property and privacy" (Nigeria Cybercrime Act, 2015, p.1).

It is very important that the proposed e-government security framework operates within the confines of established regulations. A regulatory framework here has to do with set of rules instituted by government to govern how citizens, services providers and stakeholders will use e-government systems effectively while upholding information security and privacy standards. To ensure that these rules are strictly adhered to, there must be provisions for enforcement so that defaulters will face associated penalties as a way to deterring others. These could be achieved by creating a legal framework for e-government security; a legal framework is basically putting in place a system of formal laws, conventions, procedures, norms to shape the behaviour and activities of users through legislations. An example of such legislations is the enactment of the Nigerian Electronic Transaction Act that was passed into law by the Nigerian Senate in 2015.

Framework Requirements

The framework has essential requirements to ensure that there is a secure G2G, G2C and G2B communications, securing applications, servers, hosts and networks against internal and external threats, the security is provided according to the security layers.

Securing E-Government Networks

Most security breaches in e-government occur mainly during the exchange, processing and storing of data, altering data without due authorization (Urbanczyk, 2013). Securing the e-government network is similar to traditional computer networks that utilize cryptography, PKI, firewalls and digital signatures (Mohammadi & Nikkhahan, 2009). The e-government network here means the network assets, which includes network host, interconnecting devices and data that traverses the network. Other assets are the services deployed by the government, government records and secrets. To provide adequate security, it is important to identify the essential assets that need protection and what kind of protection they

require. Security professionals recommend the security-in-depth principle. The principle declares that 'every network security should be multi-layered, applying diverse technologies in securing the network' (Oppenheimer, 2010). None of the techniques could guarantee a total resistance to all attacks; hence every technique can be followed up with an alternative in case of failure (backup plan). For example, the usage of a dedicated firewall in reducing the interaction between system resources and a packet filtering router that provides another level of defence. IP security or IPSec offers cryptographic supported authentication, confidentiality, and integrity services at the network layer. IPSec is considered to be more transparent as regards applications and protocols deployed by e-government providers (Boudriga, 2002). It typically provides secure communication between networked computers over unsecure mode of transmission, and can be used within e-government networks. By using IPSec-based virtual private networks (VPN), government departments and public businesses can reduce the costs of operation while maintaining the confidentiality of their information. It is very imperative to secure internal network components like switches, routers and cabling, these network devices must be treated as high-end and must be hardened against possible intrusion.

Intrusion Detection and Prevention System

The intrusion detection system (IDS) identifies malevolent situations and sends a notification to the network administrator through email or by logging the incidence. Intrusions can be distributed which may involve multiple attackers, while intruders may conceal their activities by sometimes installing modified versions of system monitoring and administration commands and also deleting their trails in the log files (Boudriga, 2002). The IDS is expected to detect any such guise by attackers. There are two kinds of IDS: IDS in host systems and the IDS in a Network. The IDS on a host exist primarily in a particular host and continue to monitor the host methodically while the IDS on the network monitors every single network passage visible checking these basic signs of malevolent incidences. The Intrusion Prevention

System works similarly to IDS but the IPS will reject any malicious event detected and not just reporting it (Boudriga, 2002).

Securing E-Government Applications

Providing e-security for online-web applications can be achieved either by using Public Key Infrastructure toolkits, which provide SSL/TLS support directly to the application, or installing PKI-middleware to give the SSL enough sustainability requiring security and relieves the end user from undergoing the intricacies of PKI implementation by the use of same set of tools in the applications. A PKI was developed in order to guarantee stability of client-server kind of applications like e-government (Kumar et al., 2010).

A PKI employ a combination of public-private key pair for:

1. Encryption for the confidentiality of data
2. Digital signature to ensure non-repudiation and integrity
3. Authentication achieved through a public key.

Deployment of PKI requires a combination of technology infrastructure for managing and allocating digital certificates and policies for certificate usage, distribution, certificate validity period and renewal (Dandis, 2015).

Legal, institutional and regulatory requirements are also very important. PKI technology provides critical security functions that the Internet cannot provide. These functions comprise: time stamping, certificate status services, archiving, and risk management mechanisms, they can be at the foundation of new service offerings. Well thought out policies documentations occupy a significant place in the effectiveness of PKIs (Nono, 2012; Al-Khouri, 2012).

The policy documents are:

1. Certificate Policy Document
2. Certificate Practice Statements
3. Agreements

Certificate Policy Document

CP typically describes the appropriate use for certificates, defines the classes of users of the PKI, and the inter-operation of multiple certifications authorities.

Certificate Practice Statements

CPS is a comprehensive declaration of certain of practices and procedures followed by a single certification authority (CA). It explains how the CA/PKI meets the requirements of the CP.

Agreements

An agreement between two parties defines the responsibilities of the parties, and the terms and conditions under which the parties may use issued certificates. When PKIs wish to inter-operate, PKI documentation becomes the main tool to facilitating that inter-operation. Such interoperation can establish minimum operating requirements in a CP, while cross-certification (or mutual recognition of certificates) may need compliance of the associated CPS. However, CP and CPS comparison does not necessarily determine interoperability decisions. Differing technical issues and differences in the underlying legal frames may limit easy comparison (Al-Khouri, 2012; Lambrinoudakis et al., 2003; Zhong, 2010; Alshboul, 2012)

Common practices have been that application developers focus on either testing vulnerabilities out or purely reactive security patching, with little focus on designing security in, resilience, or survivability (Diamant et al., 2015)

Survivability

In fact, survivability is a higher level concept based on traditional security infrastructure, it is concerned more about the holistic performance of the system particularly if the system can “survive” incessant threats such as attacks, system faults and accidents (Xiao et al., 2009). Most of the efforts at securing information systems such as e-government system have been basically the deployment of tools that will harden system defence with strong authentication techniques and encryption techniques. What has been left out is ensuring the survivability of the

whole e-government system in case of breaches or attacks. Though most security solutions may guard a particular layer on the network system it may sometimes bring about vulnerabilities to other layers of the network (Yurcik et al., 2009). Survivability is an advanced level of security as it includes the functionality of the whole systems infrastructure. Yurcik et al. (2009) introduced the expression "survivability-over-security" (SOS) to describe the importance of the phenomenon in information security systems.

Survivability Description and Requirements

The concept of system survivability came from the military background. It is defined as a characteristic of systems, processes or procedures that provide a definite guarantee that a thing will carry on its usual functionalities irrespective of any kind of disaster or interruption; another way to describe it is that it considers prospects of services rendered by the e-government platform and the time it takes to provide such service (Liu et al., 2004; Al-Kuwaiti et al., 2009).

The concept of survivability develops upon the reliability principle which sets out to recover the system after a disaster and most parts of the services have been disrupted. The idea behind the subject of survivability is to link security attacks and ensure their immediate restoration or recovery from such attack. The main purpose of focusing on survivability is because of the need to ensure that e-government services are uninterrupted at no time irrespective of the gravity of the failure (Yurcik et al., 2009). Juxtaposing reliability and survivability, you will see that reliability presuppose that system breakdown can be stopped completely, but survivability presumes that systems breakdown may not be completely eliminated therefore irrespective of whatever level of attack, critical e-government services will still be carried out (Yurcik et al., 2009).

Survivability seems to be the most suitable solution because it has limitless allowances for system failures and the capacity to withstand any kind of attack.

Joshi et al. (1998) therefore argues that e-government should possess the capability of a system that should fulfil or deliver its services swiftly, in the face of system

attacks or breaches. This should be the bedrock of any e-government set up, ensuring the system survives an attack.

For a system to be considered to have such a capacity there should be a program with the ability to recognise and defend against attacks, ability to recover from attacks as well as switch modes during attacks which will end up reducing the severity of such attacks.

It is expected that activities carried out by this system in an unsecured environment be categorized as essential and non-essential. Furthermore, the services expected of the system in the presence of attacks need to be prioritized and minimum operational levels specified. Therefore, it could be said that a survivability scheme can be categorised as follows:

- Defence
- Detection
- Response-Recovery

The survivability theory is applicable to all the system that provides essential services in the e-government system. The main purpose is to ensure that the essential services still work optimally until there is a full recovery from the attacks.

Fault Tolerance

Fault tolerance is a key factor in ensuring high availability and dependability of essential services during program implementation. To reduce the effect of any attack on the system, the system should have the capacity to anticipate attacks and the ability to proactively stem those attacks if they occur (Bala & Chana, 2012). Fault tolerance modus operandi is employed to foresee possible breakdown or attacks and respond swiftly and accordingly.

The security fault-tolerance approach is presented as an alternative to developing highly secure application from scratch. Security fault tolerance conforms to the idea that critical system application may contain vulnerabilities that could be exploited,

and seeks out effective means to prevent these vulnerabilities from being exploited efficiently by attackers.

The categorization is potent enough to analyse and evaluate the similarities and differences of relatively varied techniques such as program-type checking, and firewalls. The goal of security fault-tolerance techniques is for system survivability as against complete system security. However, security fault-tolerance techniques provide better security assurances compared to the traditional security technique, security fault tolerance is considered to be more cost effective, it is projected that security fault tolerance may offer a practical path to higher survivability for e-government systems (Pu & Cowan, 1998).

Description of the Strategic Framework

The processes in the framework shown in figure 6-1 are governed by the laws, regulations and policies described in section 6.4. It was designed to comply with relevant security standards such as the National Information Systems and Network Security Standards and Guidelines under the NITDA Act of 2007 as described in section 5.3. As earlier explained in section 6.3, users are expected to first of all register their verifiable credential certified by a registration authority so as to be issued with unique user identification; this unique user identity (e-identity) will be used to authenticate the user before the user can gain secure access through a secure channel. This process is necessary so that every login can be recognised, especially in situations where users escalate their access privilege. A detailed technical model of these processes which includes: servers, networks and applications as stated in section 6.5 are illustrated in figure 6-2 and further descriptions made to it in section 6.8. The reason for these security processes is to ensure that the e-government services provided adhere to the fundamental principles of information security, namely confidentiality, integrity, availability and non-repudiation. The principle of survivability has become even more important owing to the spate of cyber attacks in the world today; government businesses and processes must remain accessible in spite of underlying faults or attacks, which however is the focus of this framework. A proactive security system that has an

inherent ability to survive is described in 6.6; section 6.7 also explains the utilization of a fault-tolerant mechanism that can guarantee survivability.

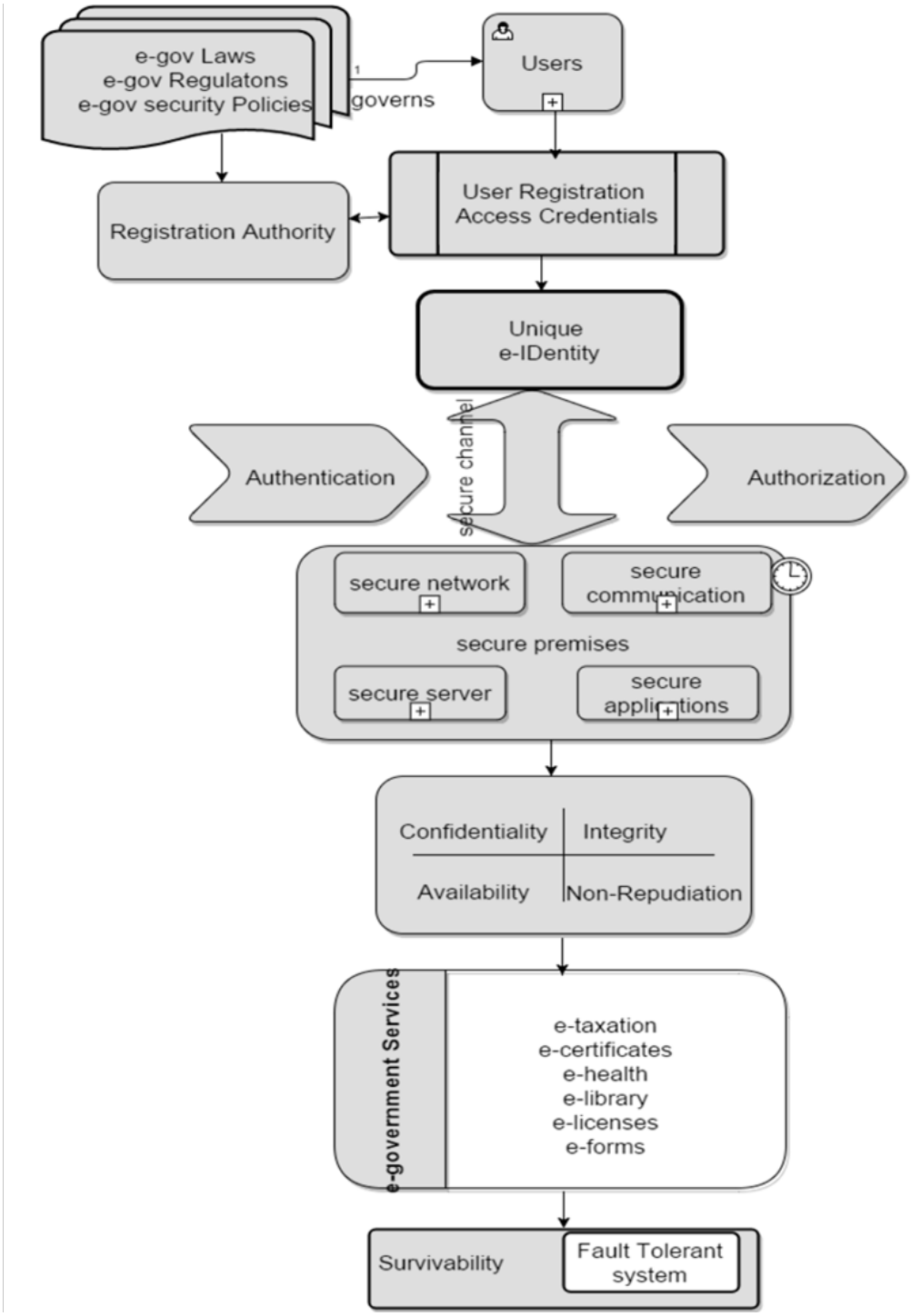


Figure 6:16 Strategic framework for e-government security

Framework Performance Model

This model shows how the e-government system relates to customers; it employs a two way certificate authentication in the authorization of valid users for respective services. After the authentication point, the user logs in to carry out a specified service. The system ensures that every communication between parties within the e-government infrastructure is encrypted. The framework recommended the utilization of a session key because of it is randomly generated, making it harder for attackers to sniff messages from the network.

The framework has what is known as the security middleware, it is basically a link between the public key infrastructure system and the applications. The whole applications function together to make sure the system is generally secure. This middleware serves as an interface between applications; manage the access control servers, the encryption tools and other critical physical mechanisms. Role based access control makes it possible for proper allocation of responsibilities in line with policies enshrined in the strategy framework, it is mostly done based on hierarchical considerations.

This makes it possible for systems administrators to dynamically manage the access of users which makes it easier for auditing, the system will report who, where and when a login was initiated as well as the duration an activity was carried out. Any valid user that elevates his access permission will also be identified and reported accordingly.

This model has an identity verification system, a backup server and a backup power system which were obvious deficiencies in previous models particularly the one presented by Zhong (2010).

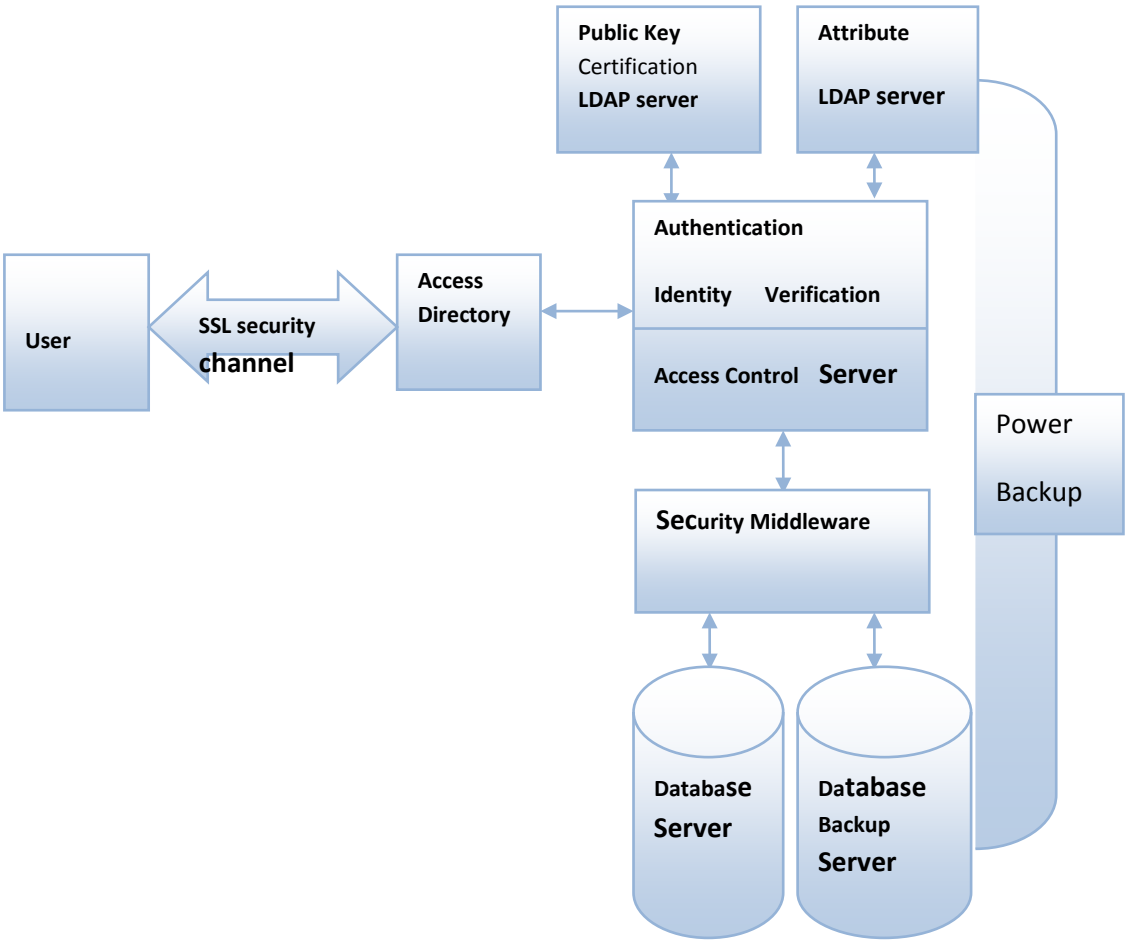


Figure 6:17 Framework performance model

Framework Evaluation

Evaluating the framework was considered a vital aspect of a framework adoption. It is a process that offers an opportunity for stakeholders to get diverse opinions on the workability or quality of the designed framework. One of the reasons for evaluation is to achieve optimal performance; therefore the processes are repeated practically to give room for possible errors so that adjustments could be made where possible. There are several evaluation methods:

- Descriptive
- Observational
- Analytical
- Testing
- Experimental

(Guba et al., 1994; Patton, 1990; Hevner et al., 2004)

Descriptive and analytical methods of evaluation seem very apt for this theory. Likewise, for practical evaluations, testing and experimental methods would have been the more suitable to adopt (Hevner et al., 2004). However, the scope of this research did not include real-world implementation of the framework in a government organisation, which would have required more time and resources.

Consequently, a questionnaire to guide the process was designed. The questionnaire had different evaluation criteria as reflected in the following questions: is the framework simple and easy to use, is the framework proactive and adaptable to respond to threats?, is the framework capable of mitigating security risks or threats that may disrupt service delivery, is the framework apt and relevant to the current maturity level as regards e-government in Nigeria, does the framework adequately address both technical and non-technical issues related to e-government security, is it considered reliable, does the framework comply with relevant laws, policies, security standards.

It may be significant to understand that because the primary reason for carrying out a framework evaluation was to get opinion of experts, use them as feedback for

possible improvements or endorsement. The research results of the ratings for those that accepted that the framework were well presented and fit for purpose indicated as either 'I strongly agree', 'I agree', Not sure' and 'Disagree'. A detailed analysis is shown in the charts subsections 6.10.1 to 6.10.7, a copy of the questions can also be found in appendix IV. The following is a summary of the framework evaluation results.

Simplicity and Ease of Use

Thirty-three out of 68 experts representing 48.5% of those that participated in the framework evaluation indicated that they strongly agreed that the framework was simple and easy to use, while 34 persons representing 50% of the experts that responded agreed that the framework was simple and easy to use. This results in a total of 98.5% of respondents supporting the position that the framework is simple and easy to use; details are shown in Table 6.2 and Figure 6-4.

Table 6:17 Responses to framework's simplicity and ease of use

Do you think the proposed framework is simple and will be easy to use by e-government stakeholders?		
Answer Options	**Response Per cent**	**Response Count**
I strongly agree	49%	33
I agree	50%	34
I am not sure	2%	1
I disagree	0%	0
	answered question	**68**
	skipped question	**0**

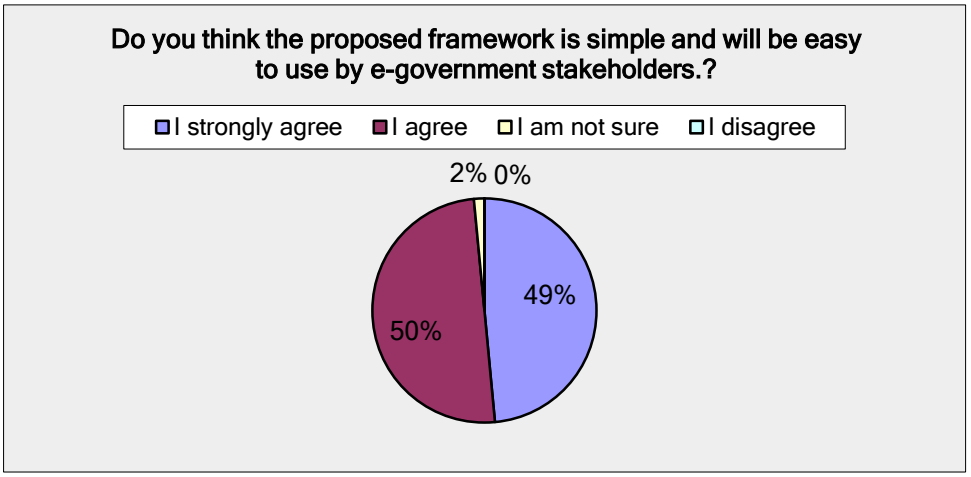


Figure 6:18 Responses to framework's simplicity and ease of use

Proactive and Adaptable

The second evaluation criterion was to determine if the framework is proactive and adaptable to respond to potential threats to e-government, out of the 68 experts that participated, 32 of them representing 47.1% said they strongly agreed that the framework is proactive and adaptable while 28 persons representing 41.2% indicated that they agree that the framework is proactive and adaptable to respond to potential threats to e-government. Also, 8 out of the 68 participants indicated that they were not sure. As a result, 88.3% of respondents endorsed that the framework is proactive and adaptable to respond to potential threats to e-government in Nigeria. Details are illustrated in Table 6.3 and Figure 6-5.

Table 6:18 Is the framework proactive and adaptable to respond to potential threats to e-government?

Is the proposed framework proactive and adaptable to respond to potential threats to e-government service delivery in Nigeria?		
Answer Options	**Response Per cent**	**Response Count**
I strongly agree	47%	32
I agree	41%	28
I am not sure	12%	8
I disagree	0%	0
answered question		**68**
skipped question		**0**

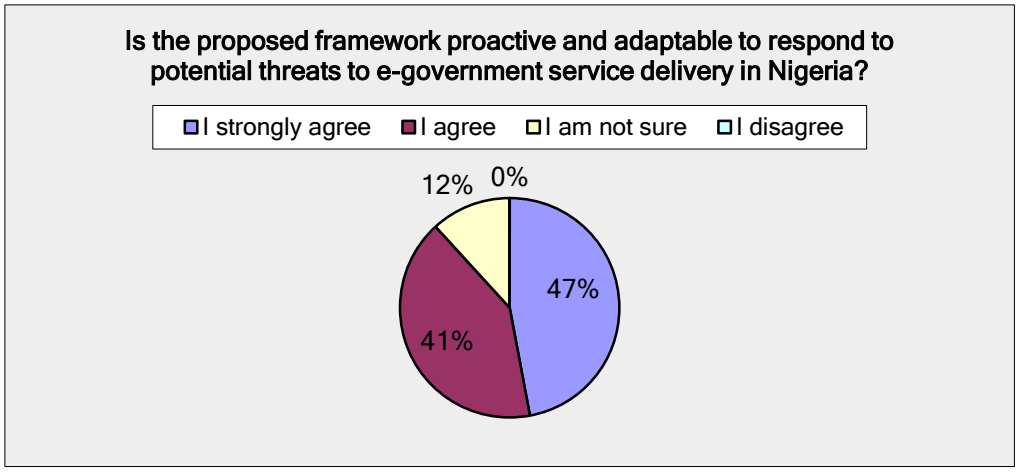


Figure 6:19 Is the framework proactive and adaptable to respond to potential threats to e-government?

Capacity to Mitigate Security Risk

Responding to the question of "if the framework has the capacity of extenuating security risk and the threats to e-government service delivery", 31 persons representing 45.6% of participants indicated that they strongly agreed that it is capable, 24 persons representing 35.3% said they agreed that the framework is capable, while 12 persons representing 17.6% indicated that they were not sure. Therefore, the conclusion according to details shown in table 6.4 and figure 6-6 is that 80.9% of the respondents confirmed that the framework has the capability to mitigate security risk and threats to e-government service delivery.

Table 6:19 Framework's capability to mitigate security risk and threats to e-government service delivery

Do you think the proposed framework is capable of mitigating security risk and threats that may disrupt e-government service delivery?		
Answer Options	**Response Per cent**	**Response Count**
I strongly agree	46%	31
I agree	35%	24
I am not sure	18%	12
I disagree	0 %	0
answered question		**67**
skipped question		**0**

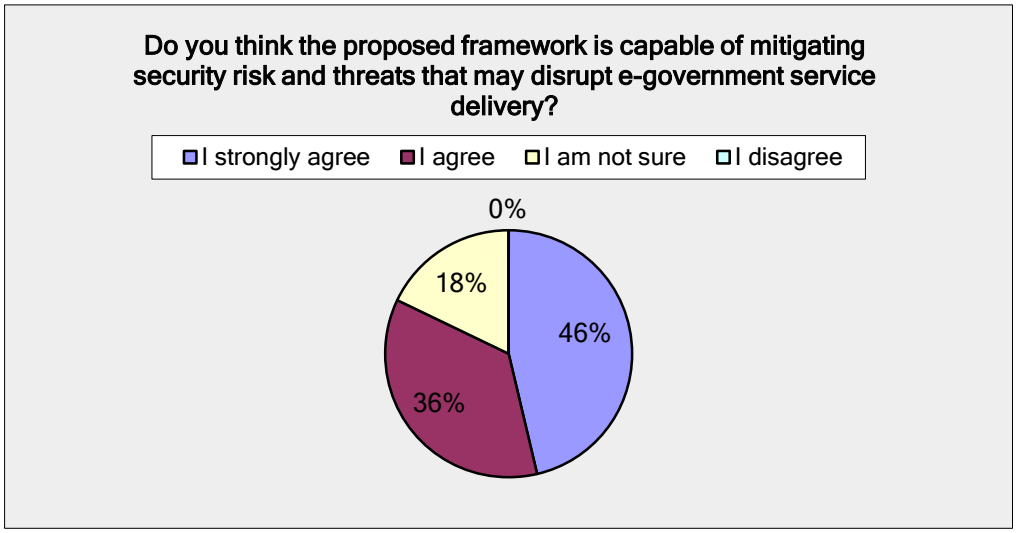


Figure 6:20 Framework's capability to mitigate security risk and threats to e-government service delivery

Relevance to Present E-Government Maturity Level in Nigeria

Is the framework apt and relevant to the present level of e-government maturity level in Nigeria? Thirty respondents representing 44.1% of participants indicated that they strongly agreed that the proposed framework is apt and relevant to the present e-government maturity level, 27 respondents representing 39.7% said they agreed, but 11 persons representing 16.2 of the respondents said they were not sure. Therefore, it is easy to conclude from the details provided in Table 6.5 and Figure 6-7 that the framework is apt and relevant to the present e-government maturity level in Nigeria because 83.8% of the respondents attested to it.

Table 6:20 Framework's relevance to the present e-government maturity level in Nigeria

Do you think the proposed framework is apt and relevant to the present e-government maturity level in Nigeria?		
Answer Options	**Response Per cent**	**Response Count**
I strongly agree	44%	30
I agree	40%	27
I am not sure	16%	11
I disagree	0%	0
answered question		**68**
skipped question		**0**

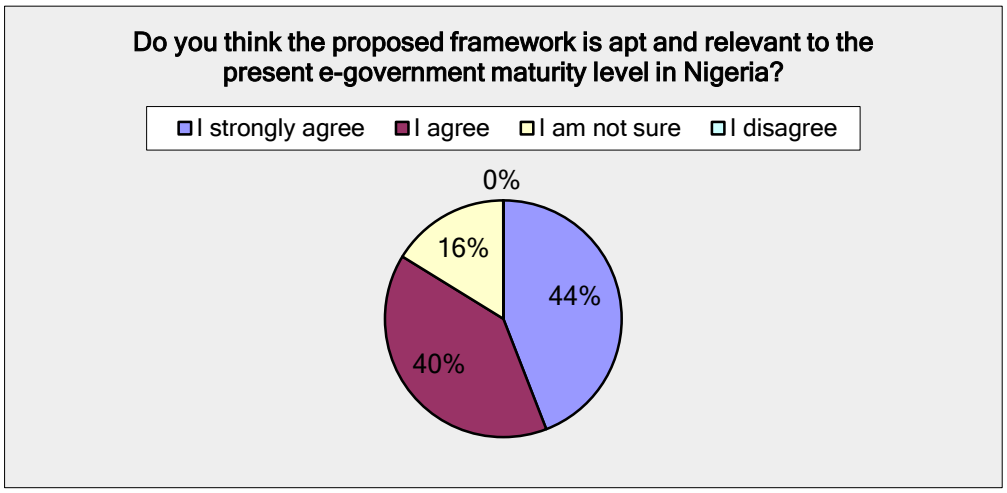


Figure 6:21 Framework's relevance to the present e-government maturity level in Nigeria

Technical and Non-Technical Issues

E-government security deals with both technical and non-technical issues. In the evaluation, the researcher sought to confirm the opinion of respondents if the framework was considered to have addressed both technical and non-technical issues in e-government security. Out of the 68 participants, 32 which represent 47.1% of the respondents said they strongly agreed that the framework did adequately address technical and non-technical issues and 28 respondents representing 41.2% indicated that they agreed to the fact that the framework

adequately addressed the technical and non-technical issues, while 8 respondents which is 11.8% of the total respondents said they were not sure. It was therefore concluded that the framework addressed all the necessary issues both technical and technical. Details of the responses are illustrated in Table 6.6 and Figure 6-8.

Table 6:21 Frameworks' adequacy in addressing both technical and non-technical issues

Do you think the proposed framework adequately addresses both technical and non-technical issues related to e-government security?		
Answer Options	**Response Per cent**	**Response Count**
I strongly agree	47%	32
I agree	41%	28
I am not sure	12%	8
I disagree	0.0%	0
answered question		**68**
skipped question		**0**

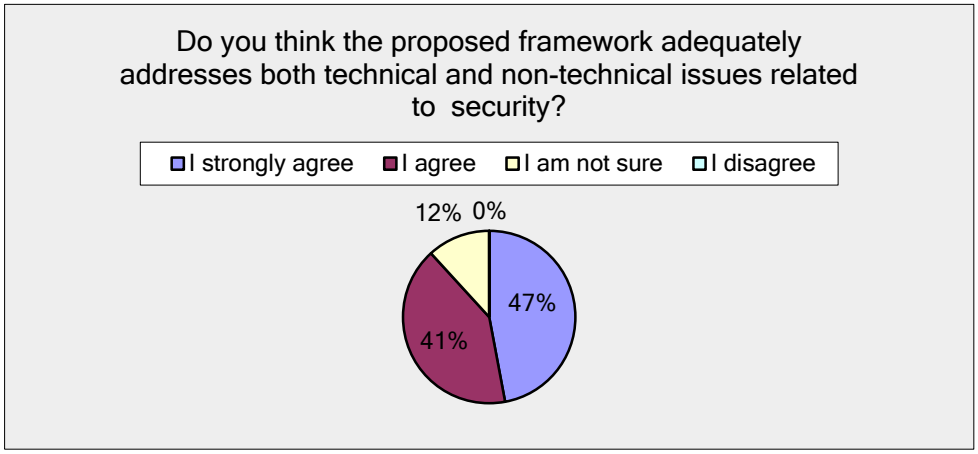


Figure 6:22 Frameworks' adequacy in addressing both technical and non-technical issues

Reliability

Is the framework considered reliable and dependable in terms of ensuring availability of e-government services? Thirty-three respondents which is 49.3% of the total participants indicated that they strongly agreed to the consideration that the framework is reliable and 25 respondents which represents 37.3% of the respondents said they agreed that the framework is reliable, while 9 respondents

representing 13.4% of the respondents said they were not sure. Therefore, it was concluded that the framework is reliable and dependable in ensuring that e-government services are always available. Details of the responses are shown in Figure 6.8 and Table 6-7.

Table 6:22 Framework's reliability in terms of ensuring availability of e-government services

Do you consider the proposed framework reliable and dependable in terms of ensuring availability of e-government services?		
Answer Options	**Response Per cent**	**Response Count**
I strongly agree	49%	33
I agree	37%	25
I am not sure	13%	9
I disagree	0%	0
answered question		**67**
skipped question		**1**

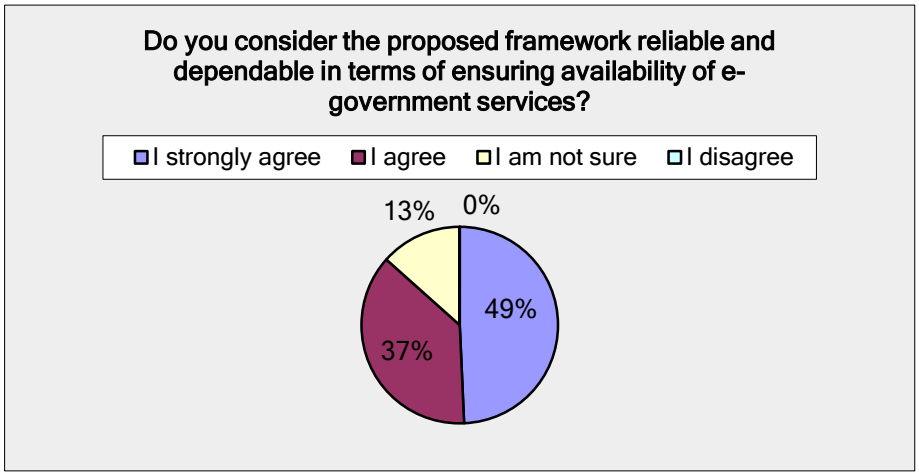


Figure 6:23 Framework's reliability in terms of ensuring availability of e-government service

Compliance with Regulations, Standards and Best Practices

The framework is expected to comply with relevant laws, regulations, standards and best practices in the industry. In this evaluation criterion, a total of 46 respondents representing 67.6% said they strongly agreed that the framework complied with relevant laws, regulations, standards and best practices, seventeen respondents

representing 25.0% of the total respondents said they agreed, while 5 respondents which is 7.4% simply said they were not sure. Accordingly, a total of 92.6% of all respondents affirmed that the framework complied with relevant laws. Details of the responses are shown in Figure 6.9 and Table 6-8.

Table 6:23 Responses on framework's compliance with relevant laws, regulations, standards and best practices

Does the proposed framework comply with relevant laws, regulations, security standards and best practices?		
Answer Options	**Response Per cent**	**Response Count**
I strongly agree	68%	46
I agree	25%	17
I am not sure	7%	5
I disagree	0%	0
answered question		**68**
skipped question		**0**

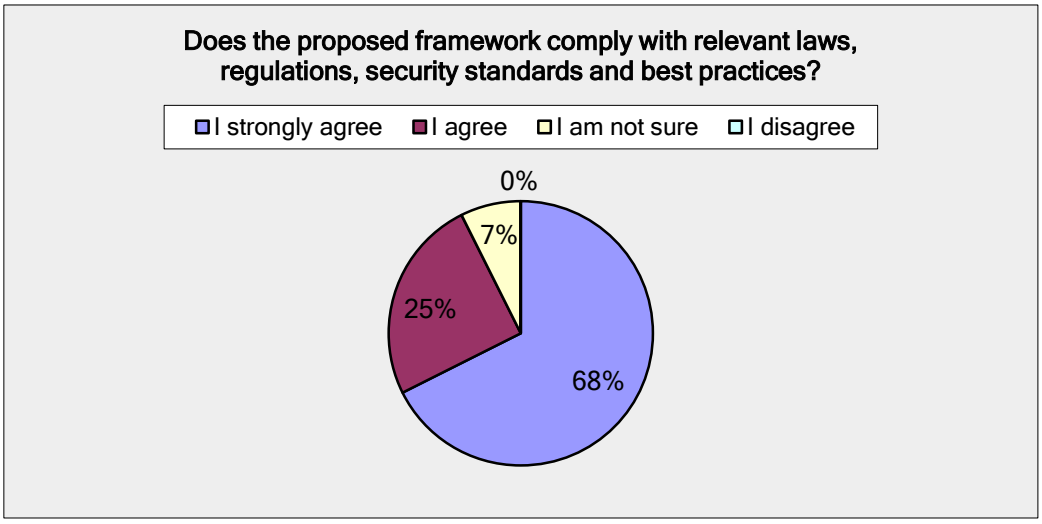


Figure 6:24 Responses on framework's compliance with relevant laws, regulations, standards and best practices

Summary

As a crucial contribution, the importance of a strategic framework was made known, also showing that a pictorial or graphical representation delivers more information at a glance than a volume of text, making a strategic framework a valuable tool to e-government policy decision-makers. The research considered that a generalised framework for e-government was not very practicable at the moment due to the fact that countries differ in so many ways, including legal systems and culture, among others.

The framework considers all aspects of e-government security: the people, the processes and the technologies; integrating these into the main framework was very strategic. It included requisite fundamentals which include: network security, host security, identity management, security components, as well legal and regulatory considerations. The framework stands out amongst contemporary research based on its strategic possession of a survivability system which relies on a fault-tolerant mechanism.

The framework design was evaluated and validated by experts in the field; these experts, as indicated earlier, are professionals in IT from the public and private sectors as well as academia. They were given the opportunity to observe and critique the framework vis-à-vis the e-government security situation in Nigeria, as demonstrated by data collected in this research. The validation was done based on selected evaluation criteria where the majority of the respondents endorsed the framework approach to addressing e-government security issues in the case study.

Conclusions and Future Work

Introduction

This chapter presents the conclusions of the whole research carried out over the last three years; it elucidates the pertinent questions addressed in the study and provides a summary of the contributions. It provides an overview and findings of the various processes or levels involved in the design of a strategic framework for e-government security in Nigeria. Attention is drawn to some research limitations and some recommendation for further studies in this area of research. This chapter highlights key achievements of this research in line with the set objectives.

Meeting the Research Aim and Objectives

All the research objectives outlined in Section 1.2.2 have been in achieved; the first objective was to carry out critical study of existing academic research on e-government security implementations and this was achieved in chapter two of this thesis. The second objective was to present a theoretical and conceptual framework for secure e-government research, which was achieved in chapter three. The third objective was to verify the primary reasons for the slow pace of e-government adoption in Nigeria and recommend a solution, which was achieved in chapter four. The fourth objective was to check compliance with existing standards, frameworks and best practices; these were achieved in chapter five. The fifth objective which was to build a strategic framework for e-government security implementation in Nigeria that will consider every aspect of e-government security, the people, the processes and the technology was achieved in chapter six. The sixth objective which was to integrate a fault-tolerant mechanism to guarantee survivability in the e-government security system was also achieved in chapter six.

All the research objectives outlined have been achieved. To accomplish these objectives, the thesis set out two clear lines of action; the first was to investigate possible reasons for the slow adoption of e-government in Nigeria, and the second was to proffer solutions or at least provide procedures towards improving the

present conditions. To accomplish these, it was however necessary to understand basic fundamentals of e-government, like the e-government implementation and maturity models, barriers and challenges facing e-government adoptions, security implications of adopting e-government by citizens, as well as carrying out a comparative analysis of the ranking of Nigeria amongst other countries by the United Nations department of economic and social affairs (UNDESA) through its division for public administration and development management (DPADM). All these were stated in chapters one, two, three and four.

Chapter four therefore specifically provided answers to the following questions through a planned data collection process:

- What are the relative preferences between e-government transactions and the traditional manual way of conducting government businesses?
- What is the present maturity level of e-government development in Nigeria?
- What is the acceptability or level of satisfaction with the current level of e-government development amongst stakeholders?
- What is responsible for the slow pace of e-government adoption in Nigeria with reference to the latest United Nations e-government survey rankings?
- Is unique identification relevant to e-government deployment in Nigeria?
- Is it vital to integrate a security framework into an e-government strategy from the outset?

The second action of the work was consequent upon the outcome of the first; it proposed solutions to the obvious concerns identified. Concerns over security, privacy and general lack of trust in the system were clearly identified. However, the proposed solution was designed to advance the speedy adoption of practices that will guarantee e-government security in conformity with relevant information security regulation, policies, frameworks and best practices in the industry. These were demonstrated in chapters five and six.

Research Approach

The research adopted the pragmatic approach due to its strategic relevance in a real-world situation, so it is an applied research that utilized both quantitative and

qualitative methods. The study utilized responses from the respondents in the initial interview to develop a questionnaire to stakeholders to enable the recording of statistical facts. Owing to the focus of the study it was aimed at getting the opinions of policy makers, citizens (users) and service providers alike. Hence, technical details and jargons were consciously minimised to avoid ambiguity for participants.

Those that responded to the questionnaires were ICT top decision-makers in the public sector, ICT top decision-makers in the private sector, ICT personnel in the public sector, ICT personnel in the private sector, and members of academia as well as general end users. There were ten questions in the questionnaire though not all the analyses are reported; the ones that are reported are those considered very relevant at this level of the study.

Nigeria runs a federal system of government, and the policy direction of the country emanates from the central government located in the Federal Capital Territory. So all the ministry departments that are responsible for e-government policies are located in the FCT, therefore the survey took place among the stakeholders there.

Findings

Most of respondents indicated that e-transactions are much more preferable compared to the traditional manual transactions in government institutions. They also provided reasons for their preference for e-transactions, describing them as more convenient, more transparent, more time efficient and that it saves cost and increase productivity. Most of the respondents indicated that they were dissatisfied with the present level of e-government development in Nigeria. Among the factors that were listed as the possible causes for the slow pace of e-government adoption in Nigeria were low computer literacy level, low Internet access, lack of confidence in government initiatives, concerns over online theft and related crimes and concerns over non-prosecution of cyber-related crimes under the present laws in case of any breach. However, most of the respondents said concerns over online theft and related online crimes could be responsible.

Most of the respondents also indicated that security and privacy were considered more and most paramount in the adoption of e-government in Nigeria. The respondents strongly recommended that a security framework should be integrated into the e-government strategy from the outset and not as an add-on in the implementation process.

Consequent on the above findings, it became more apparent that respondents wish to have an effective e-government in place. It was also very obvious that security and privacy related concerns are a major concern in the adoption of e-government in Nigeria. The questionnaire presented the question relating to security and privacy in several ways so as to measure consistencies in respondents' responses. It was confirmed that respondents were sure of what they indicated at every given instance; indeed security and privacy was a major concern that needed to be addressed by way of integrating a security framework into an e-government strategy.

The Contributions of a Security Framework

This thesis showed why it is important to have a strategy and a framework in the implementation of a secure e-government in what is described as a Strategic Framework. Having seen the relative neglect of this vital aspect, security problems that e-government needs to settle are not only what traditional government faces, but also many new situations and problems based on its own characteristics (Zhao, 2011). It will be an error to consider cyber-security and related issues as a challenge only limited to IT projects, a cyber attack can bring down government initiatives and businesses. Therefore it is very vital to initiate a very robust security strategy (Humphreys, 2013).

Absence of a proper framework that includes various aspects of e-government appears to be a gap, especially in the evaluation of IT security and privacy policies within e-government (Syamsuddin & Hwang, 2010). The framework therefore is to provide a universal underlying factor for understanding, managing, and communicating e-government security risk.

The study considered the diversities amongst nations; the study initially planned to build a generalised framework but considering some of the issues under listed, it was considered impracticable at least within the resources made available for the duration of this research.

There are some local realities in Nigeria that makes some processes rather slow due to the present legal system, cultural beliefs, political system etc. The unique identification system was examined, and there is an on-going project aimed at providing a simple database program that will be implemented in all the 774 local areas. A process where a citizen's basic information will be provided and unique local government identity will be issued based on iteration of fields in the record that will be difficult to guess. This will be done in line with local realities and in accordance with relevant laws and policies on data protection and privacy. The strategic framework was designed to function according to e-government laws, e-government regulations and policies related to e-government security in Nigeria. The government policies guide processes of the registration authority where users register and get access credentials. The framework guarantees secure authentication and authorization while also ensuring secure network, secure communications, secure server, and secure applications as well as secure premises/perimeter. With this the core values of information security confidentiality, integrity, availability and non-repudiation are achieved. Furthermore, the framework proposed a system that will continue to deliver e-government services in the face of attacks; the system has an inherent ability to survive. This is achieved through a fault-tolerant mechanism that ensures survivability of the e-government processes.

Compliance with Information Security Regulations, Policies, Standards and Frameworks

Some of the most commonly adopted standards and regulations for information security relevant to this research were discussed so as to provide relevant guidance, namely: Control Objectives for Information and related Technology (COBIT), International Organization for Standardization (ISO) 27001 and 27002 and the (US)

National Institute of Standards and Technology (NIST). In addition to that, the National Information Technology Development Agency (NITDA) guidelines were also introduced as they are very important considering the case study. E-government security frameworks by other researchers were also checked and an e-government security framework adapted to the NIST cyber-security framework was introduced as an advanced approach to mitigating security threats related with e-government. They are the framework nucleus, the framework implementation levels and the framework outline; every framework component strengthens the relationship between e-government services drivers and e-government security strategies.

Framework Validation

To validate the research, a responsive evaluation research methodology was adopted; returning to the respondents after initial identification of issues. In this case, these relevant stakeholders that participated in the initial study were given the opportunity to relate the designed framework to reality in e-government in Nigeria. A questionnaire was also used which had different evaluation criteria as reflected in the following questions: is the framework simple and easy to use, is the framework proactive and adaptable to respond to threats, is the framework capable of mitigating security risks or threats that may disrupt service delivery, is the framework apt and relevant to the current maturity level of e-government in Nigeria, does the framework adequately address both technical and non-technical issues related to e-government security, is it considered reliable, does the framework comply with relevant laws, policies and security standards.

The framework evaluation consisted of expert opinion as feedback for possible improvements or endorsement. Most of the experts strongly agreed that the framework was simple and easy to use, proactive and adaptable, has the capacity to mitigate security risk, relevant to present e-government maturity level in Nigeria, it considers both technical and non-technical issues, it is reliable and it comply with security regulations, standards and best practices.

Research Limitations

The questionnaire did not very well create an opportunity for respondents to provide subjective answers, and where there were some of these subjective inputs, those comments were not analyzed. Subsequent research should include the process of analyzing subjective responses so that it may not seem as though respondents are restricted to the researcher's assumptions.

The researcher observed some constraints and bias amongst civil servants while responding to questionnaires; some of them, to shore up the image of the administration, tended to present a positive representation of a situation that apparently was not the reality, even though the research was strictly academic. This situation could be misleading and thereby affecting the reliability of the data set. Subsequent research should take note of this situation and educate respondents to be very frank and objective in their responses.

The researcher was not in control of legislative and the policy direction in the case study, since a framework is expected to comply with relevant laws and policies of a state. At the time of the research some laws related to cyber security were passed, though policies on enforcement were still unsettled. Therefore, the study only based its projections on the existing state of things, which are subject to change as government policies are never static.

Research Contributions

The findings of this research have contributed to the e-government development literature by providing solutions to the problem relating to the slow pace of e-government adoption in Nigeria. Some of the key contributions are listed as follows:

1. This research provided evidence that online security and privacy concerns were key factors responsible for the slow pace of e-government adoption in Nigeria. It therefore initiated information security principles in the implementation of e-government.

2. The researcher developed a security framework to strengthen the connection between e-government services drivers and e-government security strategies.
3. The researcher designed a strategic framework for e-government security; the strategic framework introduced the concept of survivability through the utilization of a fault-tolerant mechanism; this is a major contribution to e-government research.

The research further stated that for an e-government system to be considered secure: the system must **survive** any form of attack; the system must **continue to deliver services**. An e-government system is too important to fail; it is like the strength of a nation, and it cannot afford downtime.

This is a vital subject for researchers, IT security experts, and policy makers in an emerging economy like Nigeria, which is considered to have a less dispersed level of e-government adoption. The discoveries and results of this research will be a useful theory for top government decision-makers at both the federal, state, local and organisational levels, it will be a guide during critical decision-making about the scaling up of e-government in Nigeria. This research contributes to e-government body of knowledge in Africa and globally, too. It will also serve as a credible reference to the government institutions in Nigeria considering full-scale implementation of e-government services. It made proposals that will guarantee secure authentication and secure transactions. There is now available data on all the research questions presented in this thesis.

The research has provided a sense of direction as to the crucial areas that require more focus in the e-government development in Nigeria; the study provided evidence about security and privacy, stating that they are major concerns in the adoption of e-government in Nigeria. This work provides a reliable reference for future researchers.

In as much as technical solutions are vital in the provision of the required security to e-government data, unscrupulous individuals may still go to extra lengths to engage in illegal transactions. Therefore, it is important to institute legislation that will

criminalise new or innovative ways of data breach in the way provided in the E-government Act of 2002 in the United States of America (E-government Act, 2002). There should be strict enforcement as well as punishment for cyber criminals.

Future Research

Future studies may look into developing this framework and processes further. This research concentrated on Nigeria; in the future, it could be extended across Africa, because Tunisia is the leading African country according to the United Nations e-government survey, Tunisia ranked 75th in the world in the 2014 survey. There could be a comparative study between the most developed country in Africa in terms of e-government adoption and Nigeria or a comparative study between Nigeria and the Republic of Korea, which is the most developed country in the world E-government Development Index. There could be a study on how culture or education influences e-government adoption amongst citizens.

However, there is no absolute security in the cyber-world, and the incessant reports of attacks show that it is no more a matter of if you are attacked but when. This research proves to be very proactive; it takes into consideration the fact that e-government contains very sensitive governmental information that may attract attackers for several reasons. The research has not only provided a guide towards resisting an attack but went further to develop mechanisms for the survivability of the e-government services and business processes even in the face of possible attacks. E-government services are so vital due its structure in guaranteeing the quality of lives of citizens; therefore it deserves the maximum security protection possible.

References

Adedayo, Butakov, S., Ruhl, R., & Lindskog, D. (2013). E-Government Web services and Security of Personally Identifiable Information in Developing Nations. In *The 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)* (pp. 623–629). Edmonton, Canada: IEEE. http://doi.org/978-1-908320-20/9

Afon, A.O, Faniran, G. . (2013). Intra-Urban Urban Pattern Of Citizens ' Participation in Monthly Environmental Sanitation Program: The Ibadan, Nigeria Experience. *Applied Sciences in Environmental Sanitation*, *8*(1), 1–10. Retrieved from http://books.openedition.org/ifra/544

Akkaya, C., Wolf, P., & Krcmar, H. (2012a). Factors Influencing Citizen Adoption of E-Government Services: A Cross-Cultural Comparison (Research in Progress). In *2012 45th Hawaii International Conference on System Sciences* (pp. 2531–2540). http://doi.org/10.1109/HICSS.2012.278

Akkaya, C., Wolf, P., & Krcmar, H. (2012b). Factors Influencing Citizen Adoption of E-Government Services: A Cross-Cultural Comparison (Research in Progress). *2012 45th Hawaii International Conference on System Sciences*, 2531–2540. http://doi.org/10.1109/HICSS.2012.278

Al-Ahmad, W., NYiT Amman, A., & Al-Kaabi, R. (2008). Analysis Security of Cyberactivism: An Extended Framework for a Case Study of Online Free Tibet Activities. In *IEEE International Conference on Intelligence and Security Informatics, 2008. ISI 2008.* (pp. 294–295). Taipei: IEEE. http://doi.org/10.1109/ISI.2008.4565091

Al-Hujran, O., Al-Debei, M. M., Chatfield, A., & Migdadi, M. (2015). The imperative of influencing citizen attitude toward e-government adoption and use. *Computers in Human Behavior*, *53*, 189–203. http://doi.org/10.1016/j.chb.2015.06.025

Al-Khouri, A. M. (2012). PKI in Government Digital Identity Management Systems.

European Journal of ePractice, *1*(14), 4–21.

Al-Khouri, A. M., & Farmer, M. (2014). A government framework to address identity, trust and security in e-government: the case of UAE management infrastructure. *European Scientific Journal*, *10*(10), 85–98.

Al-Kuwaiti, M; Kyriakopoulos, N; & Hussein, S. (2006). Network Dependability, Fault-tolerance, Reliability, Security, Survivability: A Framework for Comparative Analysis. In *The 2006 International Conference on Computer Engineering and Systems,* (pp. 282–287). Cairo: IEEE. http://doi.org/10.1109/ICCES.2006.320462

Al-Kuwaiti, M., Kyriakopoulos, N., & Hussein, S. (2009). A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability. *IEEE Communications Surveys and Tutorials*, *11*(2), 106–124. http://doi.org/10.1109/SURV.2009.090208

Al-Mayahi, I., & Mansoor, S. P. (2012). UAE E-government: SWOT analysis and TOWS Matrix. *2012 Tenth International Conference on ICT and Knowledge Engineering*, 201–204. http://doi.org/10.1109/ICTKE.2012.6408556

Al Nagi, E., & Hamdan, M. (2009). Computerization and e-Government implementation in Jordan: Challenges, obstacles and successes. *Government Information Quarterly*, *26*(4), 577–583. http://doi.org/10.1016/j.giq.2009.04.003

Alateyah, S. A., Crowder, R. M., & Wills, G. B. (2013). Identified Factors Affecting the Citizen' s Intention to Adopt E-government in Saudi Arabia. *World Academy of Science, Engineering and Technology*, *80*(8), 601–606. http://doi.org/http://dx.doi.org/10.7763/IJIMT.2014.V5.527

AlAwadhi, S., & Morris, A. (2009). Factors influencing the adoption of e-government services. *Journal of Software*, *4*(6), 584–590. http://doi.org/10.4304/jsw.4.6.584-590

Alharbi, N., Papadaki, M., & Dowland, P. (2014). Security Challenges of E-

Government Adoption Based On End Users' Perspective. In *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)* (pp. 78–82). London: IEEE. http://doi.org/10.1109/ICITST.2014.7038781

Almarabeh, T. (2010). A General Framework for E-Government: Definition Maturity Challenges, Opportunities, and Success. *European Journal of Scientific Research*, *39*(1), 29–42.

Alshboul, R. (2012). Security and Vulnerability in the E-Government Society. *Contemporary Engineering Sciences*, *5*(5), 215–226.

Alshehri, M., & Drew, S. (2010). E-Government Fundamentals. *Proceedings of the IADIS International Conference on ICT, Society and Human Beings*, (2001), 35–42.

Alsultanny, Y. A. (2014). Assessment of E-Government Weak Points to Enhance Computer Network Security. *International Journal of Information Science*, *4*(1), 13–20. http://doi.org/10.5923/j.ijis.20140401.03

Alzheimer Europe. (2009). Types of research. Retrieved July 23, 2015, from http://www.alzheimer-europe.org/Research/Understanding-dementia-research/Types-of-research/The-four-main-approaches

Andersen, K. V., & Henriksen, H. Z. (2006). E-government maturity models: Extension of the Layne and Lee model. *Government Information Quarterly*, *23*(2), 236–248. http://doi.org/10.1016/j.giq.2005.11.008

Ashaye, Olusoyi Richard, & Z. I. (2013). E-Government Implementation Benefits, Risks and Barriers in Developing Countries: Evidence from of Nigeria. In *2nd International Conference on Internet, E-Learning & Education Technologies (ICIEET 2013) joint with 2nd International Conference on Information Technology , E-Government and Applications (ICITEA 2013)* (pp. 92–105). London: IJITCS. http://doi.org/2091-1610

Asogwa, B. E. (2013). Electronic government as a paradigm shift for efficient public

services: Opportunities and challenges for Nigerian government. *Electronic Government*, *31*(1), 141–159.

Ayanso, A., Chatterjee, D., & Cho, D. I. (2011). E-Government readiness index: A methodology and analysis. *Government Information Quarterly*, *28*(4), 522–532. http://doi.org/10.1016/j.giq.2011.02.004

Azad, B., & Faraj, S. (2008). Making e-Government systems workable: Exploring the evolution of frames. *The Journal of Strategic Information Systems*, *17*(2), 75–98. http://doi.org/10.1016/j.jsis.2007.12.001

Basu, S. (2004). E-government and developing countries: an overview. *International Review of Law, Computers & Technology*, *18*(1), 109–132. http://doi.org/10.1080/13600860410001674779

Bazeley, P. (2004). Issues in Mixing Qualitative and Quantitative Approaches to Research. In *Applying qualitative methods to marketing management research* (pp. 141–156). UK: Palgrave Macmillan.

Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems*, *17*(2), 165–176. http://doi.org/10.1016/j.jsis.2007.12.002

Boudriga, N. (2002). Technical issues in securing e-government. In *IEEE International Conference on Systems, Man and Cybernetics* (Vol. 2, pp. 392–395). Yasmine Hammamet, Tunisia: IEEE. http://doi.org/10.1109/ICSMC.2002.1173444

Braun, V.; Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*, 77–101. http://doi.org//10.1191/1478088706qp063oa

Butler, J. M. (2009). Benchmarking Security Information Event Management (SIEM). Retrieved March 12, 2015, from https://www.sans.org/reading-room/whitepapers/analyst/benchmarking-security-information-event-management-siem-34755

Chen, Y. N., Chen, H. M., Huang, W., & Ching, R. K. H. (2006). E-Government

Strategies in Developed and Developing Countries: An Implementation Framework and Case Study. *Journal of Global Information Management*, *14*(1), 23–46. http://doi.org/10.4018/jgim.2006010102

Choi, J., & Chun, S. A. (2013). SecureGov: secure data sharing for government services. In *Proceedings of the 14th Annual International Conference on Digital Government Research* (pp. 127–135). Quebec City, QC, Canada. http://doi.org/10.1145/2479724.2479745

Collier, Z. A., Linkov, I., DiMase, D., Walters, S., Tehranipoor, M., & Lambert, J. H. (2014). Cybersecurity Standards: Managing Risk and Creating Resilience. *Computer*, *47*(9), 68–74. http://doi.org/10.1109/MC.2013.448

Collings, T. (2008). Some thoughts on the underlying logic and process underpinning Electronic Identity (e-ID). *Information Security Technical Report*, *13*(2), 61–70. http://doi.org/10.1016/j.istr.2008.06.002

Combass, T., & Shilling, A. (2016). Integrating Cybersecurity into NAVAIR OTPS Acquisition. In *2016 IEEE AUTOTESTCON* (pp. 1–5). IEEE. http://doi.org/10.1109/AUTEST.2016.7589632

Creswell, J. W. (2003). 'Research design, qualitative, quantitative and mixed methods approaches'. (C. Laughton, Ed.) *Research design: Qualitative quantitative and mixed methods approaches* (2nd ed.). London: Sage.

Dandis, A. T. (2015). Jordan E-Government: Security and Privacy of Information, eServices and Systems. *Jordan E-Government Program*. Jordan: Jordan E-government Program. Retrieved from http://ssc.ju.edu.jo/Documents/Jordan E-Government Security and Privacy of Information eServices and Systems (Ver. 1.0).pdf

Darren, M. M. (2011). Towards a Framework for eGovernment Development in Nigeria. *Electronic Journal of Electronic Government*, *8*(2), 147–160.

Dawes, S. S. (2008). Governance in the Information Age: A Research Framework for an Uncertain Future. In *The Proceedings of the 9th Annual International Digital*

Government Research Conference (pp. 290–297). Albaby, NY: ACM Digital Library. http://doi.org/978-1-60558-099-9

Denzin, N. K & Lincoln, Y. S. (2005). *The Handbook on Qualitative Research* (3rd ed.). Thousand Oaks, CA: Sage.

Department of Trade and Industry. (2000). Information Security: Understanding BS 7799. *Information Security*. London: DTI. Retrieved from www.dti.gov.uk/publications

Diamant, J., Misustin, J., Lazerowich, S., & Wisseman, S. (2015). Secure your critical applications. USA: Hewlett Packard Enterprise. http://doi.org/4AA5-5694ENW

DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical Education*, *40*(4), 314–321. http://doi.org/10.1111/j.1365-2929.2006.02418.x

Dillman, D. A. (2011). *Mail and Internet Surveys: The Tailored Design Method -- 2007 Update with New Internet, Visual, and Mixed-Mode Guide* (2nd ed.). Hoboken, NJ: Wiley.

Dode, R. O. (2007). Prospects of e-government implementation in Nigeria. In *Proceedings of the 1st international conference on Theory and practice of electronic governance - ICEGOV '07* (pp. 380–383). Uyo, Nigeria: ACM Digital Library. http://doi.org/10.1145/1328057.1328137

Ebrahim, Z., & Irani, Z. (2005). E-government adoption: architecture and barriers. *Business Process Management Journal*, *11*(5), 589–611. http://doi.org/10.1108/14637150510619902

European Information Society Group. (2005). *EURIM Personal Identity Secure Data Sharing as the Key to Efficiency in Service Delivery*. Westminister, UK. Retrieved from http://www.eurim.org.uk/activities/pi/DS_statusreport_Apr05.pdf

Evans, D., & Yen, D. C. (2006). E-Government: Evolving relationship of citizens and government, domestic, and international development. *Government Information Quarterly*, *23*(2), 207–235.

http://doi.org/10.1016/j.giq.2005.11.004

Federal Ministry of Communications. (2015). E-government Initiatives in Nigeria. Retrieved October 1, 2015, from http://commtech.gov.ng/index.php/department/e-government

Fielden, K. (2010). Information Security Framework. In *International Conference onInformation Society (i-Society), 2010* (pp. 25–30). London: IEEE. http://doi.org/978-0-9564263-3-8

Gamlo, A., & Bamasak, O. (2009). Towards Securing E-Transactions in E-Government Systems of Saudi Arabia. In *International Conference for Internet Technology and Secured Transactions, 2009. ICITST 2009.* (pp. 1–7). London: IEEE. http://doi.org/10.1109/ICITST.2009.5402546

Guba, E. G., & Lincoln, Y. S. (Eds.). (1994). Competing Paradigms in Qualitative Research. In *Handbook of qualitative research* (pp. 105–117). Thousand Oaks: Sage.

Gupta, B., Dasgupta, S., & Gupta, A. (2008). Adoption of ICT in a government organization in a developing country: An empirical study. *The Journal of Strategic Information Systems*, *17*(2), 140–154. http://doi.org/10.1016/j.jsis.2007.12.004

Health & Social Care Information Centre. (2002). *Registration and Authentication*. *Online*. London: Health & Social Care Information Centre. Retrieved from http://systems.hscic.gov.uk/rasmartcards/documents/raegif.pdf

Hevner, A. R., March, S. T., & Park, J. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105. http://doi.org/10.2307/25148625

Hossein Bidgoli. (2006). *HAND OF INFORMATION SECURITY. Information Warfare; Social, Legal, and International Issues; and Security Foundations* (2nd ed.). Bakersfield, California: John Wiley & Sons.

Howard, M. (2001). E-Government across the globe: How will “e” change government? *Government Finance Review*, *17*(4), 6–9.

Humphreys, E. J. (2013, October). The new cyber warfare. *International Organization for Standardization*, pp. 2013–2015. Online. Retrieved from http://www.iso.org/iso/news.htm?refid=Ref1785

International Telecommunication Union. (2009). ITU e-government Implementation Toolkit. Geneva: ITU. Retrieved from www.itu.int/ITU-D/cyb/app/docs/eGovernment toolkitFINAL.pdf

InternetLiveStatistics. (2014). Internet Users by Country (2014). Retrieved November 18, 2015, from http://www.internetlivestats.com/internet-users-by-country/

Iroegbu, S. (2016, April 19). Nigeria Loses over N127bn Annually through Cybercrime. *Thisday Newspaper*, p. 8. Abuja, Nigeria. Retrieved from http://www.thisdaylive.com/index.php/2016/04/19/nigeria-loses-over-n127bn-annually-through-cybercrime/

ISO/IEC. (2016). *International Standard ISO/IEC 27000 Information technology Security techniques - Information security management systems-Overview and vocabulary* (Vol. 2016). Online.

Jadi, Y., & Jie, L. (2014). GBC implementation strategy of E-government system for emerging countries. In *International Conference on Information Society (i-Society 2014)* (pp. 140–145). Shanghai, China: IEEE. http://doi.org/10.1109/i-Society.2014.7009028

Jayashree, S. Marthandan, G. (2010). Government to E-government to E-society. *Journal of Aplied Sciences*, *10*(19), 2205–2210.

Kalinich, K. P. (2013). *European Union cyber exposures and solutions*. *Online*. London. Retrieved from http://www.aon.com/unitedkingdom/business-risks/attachments/cyber/whitepaper-european-union-cyber-exposures-solutions.pdf

Karokola, G., Kowalski, S., & Yngström, L. (2013). Evaluating a Framework for Securing e-Government Services – A Case of Tanzania. In *2013 46th Hawaii*

International Conference on System Sciences (pp. 1792–1801). Wailea, HI, USA: IEEE. http://doi.org/10.1109/HICSS.2013.208

Krauss, S. E., & Putra, U. (2005). Research Paradigms and Meaning Making: A Primer. *The Qualitative Report*, *10*(4), 758–770. http://doi.org/10.1176/appi.ajp.162.10.1985

Kumar, S., Prajapati, R. K., Singh, M., & De, A. (2010). Security enforcement using PKI in semantic web. In *2010 International Conference on Computer Information Systems and Industrial Management Applications, CISIM 2010* (pp. 392–397). Krackow: IEEE. http://doi.org/10.1109/CISIM.2010.5643507

Lambrinoudakis, C., Gritzalis, S., Dridi, F., & Pernul, G. (2003). Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy. *Computer Communications*, *26*(16), 1873–1883. http://doi.org/10.1016/S0140-3664(03)00082-3

Layne, K., & Lee, J. (2001). Developing fully functional E-government: A four stage model. *Government Information Quarterly*, *18*(2), 122–136. http://doi.org/10.1016/S0740-624X(01)00066-1

Lean, O. K., Zailani, S., Ramayah, T., & Fernando, Y. (2009). Factors influencing intention to use e-government services among citizens in Malaysia. *International Journal of Information Management*, *29*(6), 458–475. http://doi.org/10.1016/j.ijinfomgt.2009.03.012

Lee, A. S. (1991). Integrating Positivist and Interpretive Approaches to Organizational Research. *Organization Science*, *2*(4), 342–365. http://doi.org/10.1287/orsc.2.4.342

Lin, A. C. (1998). Bridging positivist and interpretivist approaches to qualitative methods. *Policy Studies Journal*, *26*(1), 162. http://doi.org/10.1111/j.1541-0072.1998.tb01931.x

Liu, Y. (2010). The Management Perspective of Chinese E-government Security. *2010 International Conference on Electrical and Control Engineering*, 2367–

2370. http://doi.org/10.1109/iCECE.2010.584

Liu, Y., & Trivedi, K. S. (2004). A general framework for network survivability quantification. In *12th GI/ITG Conference on measuring, modelling and evaluation of computer and communication systems/ 3er Polish-German Teletraffic Symposium* (pp. 1–10). Dresden, Germany: Verlag.

Marawar, T., Kale, S., & Araspure, K. (2010). E Governance. In *DSDE 2010 - International Conference on Data Storage and Data Engineering* (pp. 183–186). Bangalore, India: IEEE. http://doi.org/10.1109/DSDE.2010.54

Metz, H. C. (2002). *Nigeria Introduction*. *The Library of Congress Country Studies*. Washington, D.C. Retrieved from https://www.loc.gov/item/92009026/

Mohammadi, S., & Nikkhahan, B. (2009). A fault tolerance honeypots network for securing E-government. In *Proceedings - 2009 International e-Conference on Advanced Science and Technology, AST 2009* (pp. 13–17). Dajeon: IEEE. http://doi.org/10.1109/AST.2009.12

Moon, M. J. (2002). The Evolution of E-Government among Municipalities: Rhetoric or Reality? *Public Administration Review*, *62*(4), 424–433. http://doi.org/10.1111/0033-3352.00196

Moosa, A., & Alsaffar, E. M. (2008). Proposing a hybrid-intelligent framework to secure e-government web applications. *Proceedings of the 2nd International Conference on Theory and Practice of Electronic Governance - ICEGOV '08*, 52. http://doi.org/10.1145/1509096.1509109

National Information Technology Development Agency. (2013). *National Information Systems And Network Security Standards & Guidelines* (version 3). Abuja, Nigeria.

NationsOnlineProject. (2015). Adminstrative Map of Nigeria. Retrieved October 1, 2015, from http://www.nationsonline.org/oneworld/map/nigeria-political-map.htm

Newman, R. C. (2006). Cybercrime, Identity Theft, and Fraud: Practicing Safe

Internet - Network Security Threats and Vulnerabilities. In *InfoSecCD '06 Proceedings of the 3rd annual conference on Information security curriculum development* (pp. 68–78). Kennesaw, Georgia: ACM Digital Library. http://doi.org/10.1145/1231047.1231064

Nigeria Cybercrime Act. Cybercrimes (Prohibition, Prevention Act, 2015) (2015). NIgeria.

NIST. (2014a). *Framework for Improving Critical Infrastructure Cybersecurity*. *National Institute of Standards and Technology*. Online. Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

NIST. (2014b). *Security and Privacy Controls for Federal Information Systems and Organizations* (800 No. 53). *Sp-800-53Ar4*. Online. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Nkohkwo, Q. N., & Islam, M. S. (2013). Challenges to the Successful Implementation of e-Government Initiatives in Sub-Saharan Africa: A Literature Review. *Electronic Journal of E-Government*, *11*(2), 253–267.

Nkwe, N. (2012). E-government: challenges and opportunities in Botswana. *International Journal of Humanities and Social Science*, *2*(17), 39–48. Retrieved from http://www.ijhssnet.com/journals/Vol_2_No_17_September_2012/5.pdf

Nono, B. (2012). *Proposing a government PKI framework for Bhutan: a soloution to e-government security requirements*. Korea Advanced Institute of Science and Technology,Yuseong-gu, Daejeon, South Korea.

Oates, B. J. (2006). *Researching Information Systems and Computing.* (1st ed.). London: Sage.

Omer, N., Elssied, F., Ibrahim, O., Adil, A., & Yousif, A. (2011). Review Paper: Security in E-government Using Fuzzy Methods. *International Journal of Advanced Science and Technology 37, December, 2011*, *37*(9), 99–112.

Oppenheim, A.N. (2000). *Questinnaire Design, Interviewing and Attitude*

Measurement (New Edition). London: Continuum.

Oppenheimer, P. (2010). *Top-Down Network Design* (3rd ed.). Indianapolis: Cisco Press.

Patton, M. (1990). Qualitative Evaluation and Research Methods. In *Qualitative Evaluation and Research Methods* (4th ed., pp. 169–186). Beverly Hills, CA: Sage.

Pu, C., & Cowan, C. (1998). System survivability through security bug tolerance. *Proceedings Third IEEE International High-Assurance Systems Engineering Symposium (Cat. No.98EX231)*, 1. http://doi.org/10.1109/HASE.1998.731601

Rabaiah, A., & Vandijck, E. (2009). A Strategic Framework of e-Government: Generic and Best Practice. *Electronic Journal of E-Government*, *7*(3), 241–258.

Rajasekar, S., & Philominathan, P. (1994). Research Methodology. *The Journal of Mathematical Behavior*, *13*(2), 239. http://doi.org/10.1016/0732-3123(94)90027-2

Reddick, C. G. (2004). A two-stage model of e-government growth: Theories and empirical evidence for U.S. cities. *Government Information Quarterly*, *21*(1), 51–64. http://doi.org/10.1016/j.giq.2003.11.004

Reddick, C. G. (Ed.). (2010). Citizens and E-Government: Evaluating Policy and Management: Evaluating Policy and Management. In *Citizens and E-government* (illustrate, pp. 207–220). Florida: IGI Global.

Rees, J., Bandyopadhyay, S., & Spafford, E. (2003). PFIRES: a policy framework for information security. *Communications of the ACM*, *46*(7), 101–106. http://doi.org/10.1145/792704.792706

Rehman, M., & Esichaikul, V. (2011). Factors influencing the adoption of e-government in Pakistan. In *2011 International Conference on E-Business and E-Government, ICEE2011 - Proceedings* (pp. 7958–7961). Shanghai, China: IEEE. http://doi.org/10.1109/ICEBEG.2011.5887093

Research Directorate of Immigration and Refugee Board of Canada. (2014). Nigeria

Issuance of National ID. Ottawa, Canada: Research Directorate of Immigration and Refugee Board of Canada. Retrieved from http://www.refworld.org/docid/48d2237734.html %5Baccessed 28 May 2014%5D

Rhodes-Ousley, M. (2013). *Information Security: The Complete Reference* (2nd ed.). New York: McGraw Hill Education.

Rorissa, A., & Demissie, D. (2010). An analysis of African e-Government service websites. *Government Information Quarterly*, *27*(2), 161–169. http://doi.org/10.1016/j.giq.2009.12.003

Rouse, M. (2015). What is a Framework? TechTarget: Retrieved April 23, 2015, from http://whatis.techtarget.com/definition/framework

Safari, H., Haki, K., Mohammadian, A., Farazmand, E., Khoshsima, G., & Moslehi, A. (2004). eGovernment Maturity Model (eGMM). *ICEIS 2004:Software Agents and Internet Computing*, *14*(17).

Sanchez-Martinez, D., Marin-Lopez, I., Gomez-Skarmeta, A. F., & Jimenez-Garcia, T. (2008). Towards e-Government: The security SOA approach of the University of Murcia. *2008 Third International Conference on Digital Information Management*, 813–818. http://doi.org/10.1109/ICDIM.2008.4746840

SANS. (2014). Information Security Policy Templates. Retrieved September 30, 2015, from http://www.sans.org/security-resources/policies

Sattarova Feruza, Y., & Kim, T. H. (2007). IT security review: Privacy, protection, access control, assurance and system security. *International Journal of Multimedia and Ubiquitous Engineering*, *2*(2), 17–32.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students*. *Research methods for business students* (5th ed.). Harlow, England: Prentice Hall.

Schwester, R. (2009). Examining the Barriers to e-Government Adoption. *Electronic Journal of E-Government*, *7*(1), 113–122.

Setiadi, F., Sucahyo, Y. G., & Hasibuan, Z. A. (2013). Balanced E-Government Security Framework: An Integrated Approach to Protect Information and Application. In *2013 International Conference on Technology, Informatics, Management, Engineering & Environment (TIME-E 2013)* (pp. 95–98). Bandung, Indonesia: IEEE. http://doi.org/10.1109/TIME-E.2013.6611971

Shahintash, Ali Hajiyev, Y. (2014). e-Government Services Vulnerability. In *IEEE 8th International Conference on Application of Information and Communication Technologies (AICT), 2014* (pp. 1–5). Astana: IEEE. http://doi.org/10.1109/ICAICT.2014.7035990

Siau, K & Long, Y. (2005). Synthesizing e-government stage models – a meta-synthesis based on meta-ethnography approach. *Industrial Management & Data Systems*, *105*(4), 443–458.

Singh, S., & Karaulia, D. S. (2011). E-Governance: Information Security Issues. In *International Conference on Computer Science and Information Technology (ICCSIT'2011)* (pp. 120–124). Pattaya, Thailand: Planetary Scientific Research Centre(PSRC).

Skopik, F., Wurzenberger, M., Settanni, G., & Fiedler, R. (2015). Establishing National Cyber Situational Awareness through Incident Information Clustering. In *2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1–8). London: IEEE. http://doi.org/10.1109/CyberSA.2015.7166126

States, C. of the U. (2002). The E-government Act. U.S Public Law.

Syamsuddin, I., & Hwang, J. (2010). A New Fuzzy MCDM Framework to Evaluate E-Government Security Strategy State Polytechnic of Ujung Pandang , Republic of Indonesia. In *4th International Conference on Application of Information and Communication Technologies (AICT), 2010* (pp. 1–5). Tashkent: IEEE. http://doi.org/10.1109/ICAICT.2010.5612065

Teniola, E. (2014, June). The Origin of the Presidential System of Government in

Nigeria. *NigerianMuse*, p. 1. Lagos. http://doi.org/20140601015318zg

Trcek, D. (2003). An integral framework for information systems security management. *Computers & Security*, *22*(4), 337–360.

Tsui, H. D., Lee, C. Y., & Yao, C. B. (2010). E-Gov.com: Outsourcing government. *Proceedings - 3rd International Conference on Information Sciences and Interaction Sciences, ICIS 2010*, 572–576. http://doi.org/10.1109/ICICIS.2010.5534763

United Department for Economic and Social Affairs. (2014). *E-government Survey, 2014*. New York. Retrieved from publicadministration.un.org/egovkb/portals/egovkb/documents/un/2014-survey/e-gov_complete_survey-2014.pd

United Nations Public Administration Network. (2013). Nigeria: Addressing Insecurity, Governance with Information Technology Tools.Retrieved December 23, 2013, from http://www.unpan.org/Library/MajorPublications/UNEGovernmentSurvey/PublicEGovernanceSurveyintheNews/tabid/651/mctl/ArticleView/ModuleId/1555/articleId/38473/Default.aspx

Urbanczyk, W. (2013). How the Implementation of New Network Technologies Influenced the Changes of E-Govemment Federal Data Centers. In *2013 International Conference on Sensor Network Security Technology and Privacy Communication System (SNS & PCS)* (pp. 53–57). Harbin, China: IEEE.

Walsh, S. (2014, May). Battle New Threats. *British Computer Society*, Retrieved July 23, 2015 from http://www.bcs.org/content/conWebDoc/52832

Wang, J. (2009). E-government Security Management: Key Factors and Countermeasure. *2009 Fifth International Conference on Information Assurance and Security*, 483–486. http://doi.org/10.1109/IAS.2009.146

Weerakkody, V., El-Haddadeh, R., Sabol, T., Ghoneim, A., & Dzupka, P. (2012). E-government implementation strategies in developed and transition economies:

A comparative study. *International Journal of Information Management*, *32*(1), 66–74. http://doi.org/10.1016/j.ijinfomgt.2011.10.005

Wimmer, M. &, & Bredow, B. Von. (2002). A Holistic Approach for Providing Security Solutions in e-Government. In *Proceedings of the 35th Hawaii International Conference on System Sciences* (pp. 1715–1724). Linz Univ., Austria: IEEE. http://doi.org/10.1109/HICSS.2002.994083

Xiao, L., Li, Z., Zhang, Y., & Wang, M. (2009). Survivability of network information system: An overview. *Proceedings of the 1st International Workshop on Education Technology and Computer Science, ETCS 2009*, *2*, 931–935. http://doi.org/10.1109/ETCS.2009.471

Yaqub, J O;Bello, H.T; Adenuga, I.A;& Ogundeji, M.O. (2013). The Cashless Policy in Nigeria: Prospects and Challenges. *International Journal of Humanities and Social Science*, *3*(3), 200–212.

Yurcik, W. (2009). Survivability-Over-Security:Providing Whole System Assurance. In *Information Survivabilty Workshop* (pp. 1–4). Urbaba, IL. http://doi.org/10.1.1.23.9573

Zhang, W. (2010). E-government information security: Challenges and recommendations. *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*, V15-1-V15-4. http://doi.org/10.1109/ICCASM.2010.5622484

Zhao, D. (2011). On several major issues of the construction of Chinese E-government information security system. *Proceedings of the 2011 International Conference on Business Computing and Global Informatization, BCGIn 2011*, 274–277. http://doi.org/10.1109/BCGIn.2011.77

Zhong, W. (2010). Research on E-Government Security Model. *2010 International Conference on E-Business and E-Government*, 699–702. http://doi.org/10.1109/ICEE.2010.182

Zuccato, A. (2005). A decision matrix approach to prioritize holistic Information,

requirements in e-commerce. In *20th Ubiquitous; security conference – security and privacy in the age of 2005; computing. IFIP TC 11;*

Zuccato, A. (2007). Holistic security management framework applied in electronic commerce. *Computer & Security*, *26*, 256–265. http://doi.org/doi:10.1016/j.cose.2006.11.003

APPENDIX I: Transcript of interview

Interviewer: Sam Deekue

Respondent: [redacted]

Place: Ministry of Communication, Federal Capital Territory, Abuja

Time: 13:20-14:00

Date: 20/12/2013

Introduction:

My name is Sam Deekue, I am a PhD student from the University of Bedfordshire, United Kingdom. This interview is part of the data collection in my research process. All the views expressed during this interview are strictly for research purposes and will be treated as confidential, so feel free to express your candid opinion on the subject.

Interviewer: Do you prefer e-government transactions to the traditional manual transactions in government transaction?

Respondent: *I will say yes, the reason been that e-government makes it easier for transactions to be completed faster than going physically to offices to carry out a particular transaction. It reduces the stress of travelling to different locations just to carry a simple task, so doing it online is better. Electronic transactions generally safes time, since it can be done from multiple locations at the same time; one may not necessarily go to the government office to carry out a transaction. Which means it is a more convenient way to carry out government transactions. I prefer it to the manual system*.

Interviewer: Are you satisfied with the present level of e-government in Nigeria?

Respondent: *Some agencies like the federal road safety commission has improved their e-services in issuing driving licenses, but generally the e-government situation is not satisfactory, the nation is yet to get there. There are a lot of improvements to make, at this pace we are not competing at all. There are a lot of government agencies that has not developed fully transactional e-government, some of them you will only see information and news about the agency, and I believe it needs*

improvement. Up till this moment there are no legal or regulatory framework for secure online transaction, citizens in my opinion may not have confidence to divulge their sensitive details on insecure government websites, particularly when they are aware that there are no straight forward penalties for cases related to online crimes. Citizens do not trust that government institutions are serious about e-services, when there is palpable lack of confidence in the leadership of the country it also affects citizens responses to the government's programs or initiatives

Interviewer: What do you think may be responsible for the slow pace of e-government adoption by Nigeria?

Respondent: *Several factors, I think the government is not showing much political will to implement e-government and as such citizens are not taking the initiative very seriously. There are no laws governing data breaches and theft, e-government is a good program but I doubt if Nigeria is really ready for a full scale implementation so far. Up till this moment there are no legal or regulatory framework for secure online transaction, citizens in my opinion may not have confidence to divulge their sensitive details on insecure government websites, particularly when they are aware that there are no straight forward penalties for cases related to online crimes. Citizens do not trust that government institutions are serious about e-services, when there is palpable lack of confidence in the leadership of the country it also affects citizens responses to the government's programs or initiatives*

Interviewer: Do you consider security and privacy as paramount in the adoption of e-government in Nigeria?

Respondent: *Yes, information security is very critical. In this age and time one cannot talk about online transactions without taking into cognizance the issue of security. Security technology must be applied at every relevant stage of e-government development if you want it to survive. It is really paramount, in this day of cyber espionages, government has to consider online security as a key component*

of the e-government system; it should be treated as a responsibility and not an option.

Interviewer: Will you recommend that a security framework be included in the e-government implementation strategy from the outset?

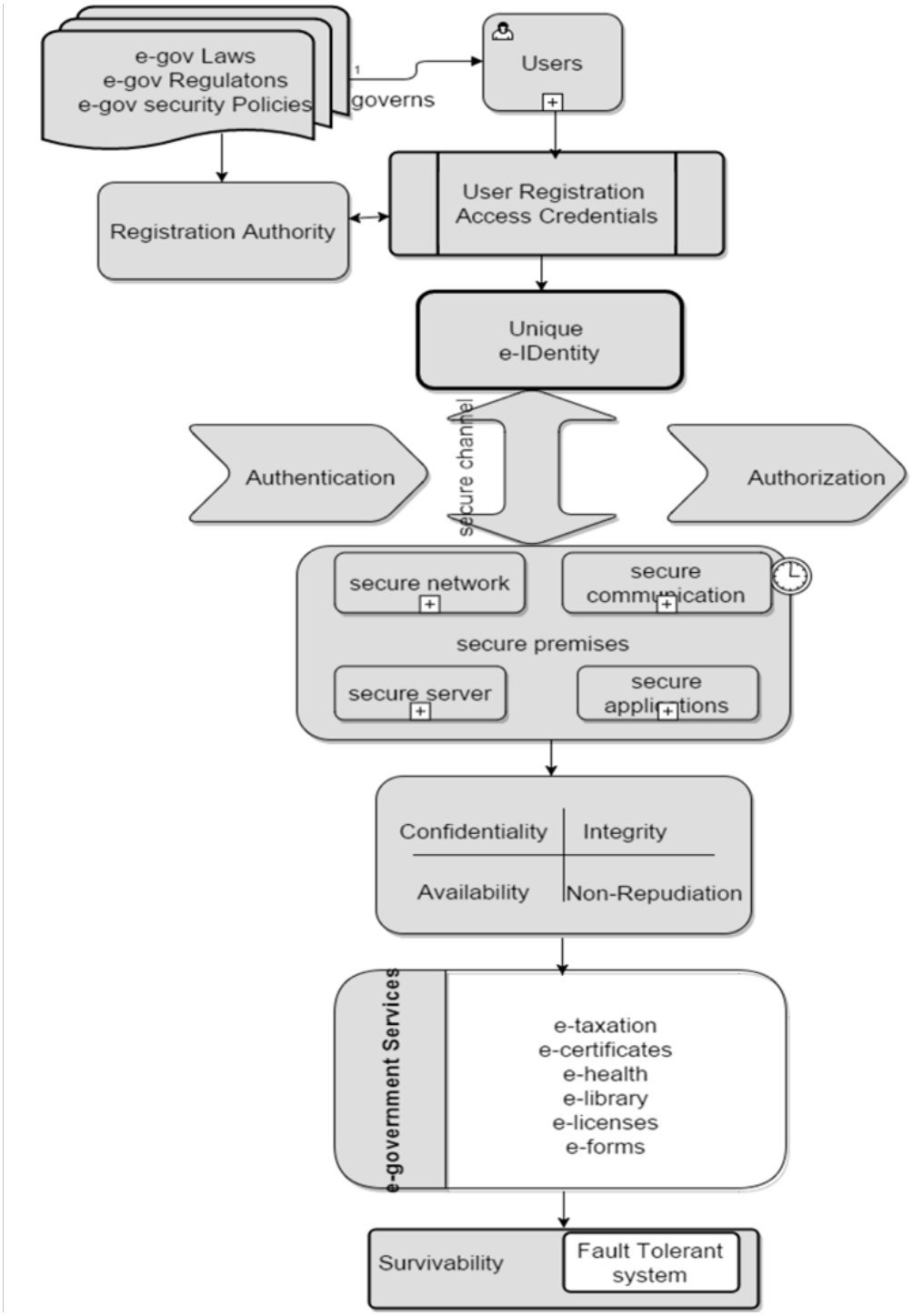
Respondent: *In the design yes, while planning for e-government implementation, there should be a plan to have robust security architecture for purposes of efficiency. The entire project may fail if there are no security plans, also regulations on e-government security has to be put in place, if it is already in existence, there should be strict enforcement because online transaction is somewhat new, Nigeria and most developing countries are not very conversant with the technology, therefore making criminal minded individuals tend to exploit the system for selfish gains.*

APPENDIX II: Table of Initial Codes

S/N	Data extract	Coded for
1	**Respondent:** By and large, electronic transactions safes time, since it can be done from multiple locations at the same time; one may not necessarily go to the government office to carry out a transaction. Which means it is a more convenient way to carry out government transactions. I prefer it to the manual system.	It safes time More convenient Prefers e-government to manual
	Respondent: I can't say I am absolutely satisfied, I can say the e-government in Nigeria is still emerging, but there are potentials for growth in the area.	Not satisfied Potential for growth
	Respondent: In my opinion, the reasons are multifaceted, there are no adequate IT infrastructure, awareness is not sufficient, low internet access as well as concerns over sensitive data protection, citizens are not too confident about online transactions due to several reports about data breaches in the news. There is low confidence in e-government system to guarantee privacy.	Reasons for slow e-gov adoption No guarantee of privacy
	Respondent: I consider security and privacy very paramount as a lot of sensitive personal details are involved in e-government transactions; it could be my medical data or tax returns. I would not want unauthorized	The importance of security and privacy Unauthorized access

	persons to have access to my details. **Respondent:** I will definitely; I believe that the importance of security and privacy cannot be over emphasized in the implementation of e-government. In every process, the security implication must be considered and tackled proactively not reactionary. Not when there is an attack that people will begin to run helter-skelter, there should be deliberate security plans, policies and strategies.	Recommend the integration of a security framework

APPENDIX III: Strategic framework for e-government security



APPENDIX IV: Questions used for framework evaluation

Acceptability Rating for Proposed Framework

Acceptability Rating for the proposed framework for e-government security in Nigeria.

You are expected to rate the framework base on the following criteria:
1. Clarity and Ease of Use
2. Comprehensiveness
3. Flexibility and Adaptability of the Framework
4. Capability and Practicability of the Framework
5. Relevance to the Nigerian Situation
6. Reliability Criterion
7. Compliance to Information Security Standards and Best Practices

Your responses are very important.Thank you for participating in this study.

1. Do you think the proposed framework is simple and will be easy to use by e-government stakeholders.?

- [x] I strongly agree
- [ ] I agree
- [ ] I am not sure
- [ ] I disagree

2. Is the proposed framework proactive and adaptable to respond to potential threats to e-government service delivery in Nigeria?

- [x] I strongly agree
- [ ] I agree
- [ ] I am not sure
- [ ] I disagree

3. Do you think the proposed framework is capable of mitigating security risk and threats that may disrupt e-government service delivery?

- [ ] I strongly agree
- [x] I agree
- [ ] I am not sure
- [ ] I disagree

4. Do you think the proposed framework is apt and relevant to the present e-government maturity level in Nigeria?

- [x] I strongly agree
- [ ] I agree
- [ ] I am not sure
- [ ] I disagree

5. Do you think the proposed framework adequately addresses both technical and non-technical issues related to e-government security?

- [ ] I strongly agree
- [x] I agree
- [ ] I am not sure
- [ ] I disagree

6. Do you consider the proposed framework reliable and dependable in terms of ensuring availability of e-government services?

- [x] I strongly agree
- [ ] I agree
- [ ] I am not sure
- [ ] I disagree

7. Does the proposed framework comply with relevant laws, policies, security standards and best practices?

- [ ] I strongly agree
- [x] I agree
- [ ] I am not sure
- [ ] I disagree

My observation is that you do clearly show where & how government policies and laws may influence e-government security implementation in the framework. If you can include that in your framework design as